

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-051439

(43)Date of publication of application : 20.02.1998

(51)Int.Cl.

H04L 9/10

G09C 1/00

H04L 9/08

H04L 9/32

(21)Application number : 09-129972

(71)Applicant : MATSUSHITA ELECTRIC IND
CO LTD

(22)Date of filing : 20.05.1997

(72)Inventor : MATSUZAKI NATSUME
HARADA TOSHIHARU
TATEBAYASHI MAKOTO

(30)Priority

Priority number : 08126751 Priority date : 22.05.1996 Priority country : JP

(54) CRYPTOGRAPHIC EQUIPMENT

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a cryptographic equipment provided with a small scale cryptographic IC and having a required minimum function to ensure security for inter-equipment communication.

SOLUTION: A 1st cryptographic IC 54 in a 1st equipment 51 combines a random number R3 generated in the process (steps 1, 3, 6, 7) to verify a 2nd equipment 52 with a random number RR4 acquired in the process (steps 2, 4, 5, 8) to prove its own validity to the 2nd equipment 52 so as to generate a time changing data transfer key (step 9) are digital literary works are cryptographer by using the data transfer key and the cryptographic data are transferred to the 2nd equipment 52 (step 11).

LEGAL STATUS

[Date of request for examination] 02.04.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3898796

[Date of registration] 05.01.2007

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] A 1st random-number generation means to be encryption equipment with which the device which performs share-izing of a data transfer key and cryptocommunication using the data transfer key is equipped, and to generate the 1st random number for share-izing of said data transfer key, A 1st random-number maintenance means to hold the 1st random number generated by said 1st random-number generation means, A 1st transmitting means to transmit the 1st random number generated by said 1st random-number generation means to the phase hand-loom machine of said cryptocommunication, the 1st random number held at said 1st random-number maintenance means -- using -- the time -- said strange data transfer key -- generating -- data transfer -- a key -- generation -- a means -- It has a transfer data encryption means to encipher using said data transfer key to the transfer data set as the object of cryptocommunication. Said 1st random-number generation means, said 1st random-number maintenance means, said data transfer key generation means, and said transfer data encryption means It is encryption equipment which is realized in the circuit in one IC and characterized by said 1st random-number maintenance means holding said 1st random number to the field which cannot be accessed from the outside of said IC.

[Claim 2] It is encryption equipment according to claim 1 which said encryption equipment is equipped with a 1st encryption means encipher further the 1st random

number generated by said 1st random-number generation means, and said 1st encryption means is realized in the circuit in said IC, and is characterized by for said 1st transmitting means to transmit the 1st random number enciphered with said 1st encryption means to said phase hand-loom machine.

[Claim 3] Said device is what said phase hand-loom machine attests mutually that it is a just device with by the communication link based on the Challenge Handshake Authentication Protocol of a challenge response mold. A 2nd random-number generation means by which said encryption equipment generates further the 2nd random number for challenge data transmitted to said phase hand-loom machine, It judges whether the response data answered from said phase hand-loom machine to said challenge data and said 2nd random number are in agreement. It is encryption equipment according to claim 2 which is equipped with an authentication means to attest with said phase hand-loom machine being a just device when in agreement, and is characterized by said data transfer key generation means generating said data transfer key when said authentication is made.

[Claim 4] Said 2nd random-number generation means and said authentication means are encryption equipment according to claim 3 characterized by realizing in the circuit besides said IC.

[Claim 5] A decryption means by which said encryption equipment decrypts the enciphered joint data which have been sent from said phase hand-loom machine further, A separation means to divide the decrypted joint data into the 1st separation data equivalent to response data, and the 2nd separation data which remain, It has a 2nd transmitting means to answer said phase hand-loom machine in said 1st separation data. Said 1st encryption means Said 1st random number and said 2nd random number are combined, and the joint data obtained as a result are enciphered. Said data transfer key generation means By combining said 1st random number and said 2nd separation data, it is encryption equipment according to claim 4 which generates said data transfer key and is characterized by realizing said decryption means and said separation means in the circuit in said IC.

[Claim 6] A 2nd transmitting means for said encryption equipment to use said 2nd random number as challenge data further, and to transmit to said phase hand-loom machine, A decryption means to decrypt the enciphered joint data which have been sent from said phase hand-loom machine, It has a separation means to divide the decrypted joint data into the 1st separation data equivalent to response data, and the 2nd separation data which remain. Said authentication means Said decision and authentication are carried out as response data answered from said phase hand-loom machine in said 1st separation data. Said 1st encryption means The challenge data transmitted from said phase hand-loom machine and said 1st random number are combined, and the joint data obtained as a result are enciphered. Said data transfer key generation means By combining said 1st random number and said 2nd separation data, it is encryption equipment according to claim 4 which generates said data

transfer key and is characterized by realizing said decryption means and said separation means in the circuit in said IC.

[Claim 7] The algorithm of encryption by said transfer data encryption means is encryption equipment according to claim 5 or 6 characterized by being the same as that of at least one thing of said 1st encryption means and said decryption means.

[Claim 8] The algorithm of encryption by said transfer data encryption means is encryption equipment according to claim 5 or 6 which differs from anything of said 1st encryption means and said decryption means, and is characterized by being simpler than which thing.

[Claim 9] Said transfer data encryption means is encryption equipment according to claim 8 characterized by enciphering said transfer data using the part to which said data transfer key corresponds to the block of fixed length to a break and each block.

[Claim 10] Said transfer data encryption means is encryption equipment according to claim 9 characterized by performing said encryption by taking the exclusive OR of said block and part to which said data transfer key corresponds.

[Claim 11] The code in said 1st encryption means and a decryption with said decryption means are encryption equipment according to claim 10 characterized by being the same conversion algorithm.

[Claim 12] It is encryption equipment according to claim 11 characterized by for said 1st encryption means and said decryption means performing said encryption and decryption using the key data beforehand held in said IC, storing a part of the key data in the mask-ROM field in said IC, and storing the part which remains in the postscript ROM field in said IC.

[Claim 13] Said device is what said phase hand-loom machine attests mutually that it is a just device with by the communication link based on the Challenge Handshake Authentication Protocol of a challenge response mold. A decryption means by which said encryption equipment decrypts the enciphered joint data which have been sent from said phase hand-loom machine to said challenge data further, A separation means to divide the decrypted joint data into the 1st separation data equivalent to response data, and the 2nd separation data which remain, An authentication means to judge whether said 1st random number and said 1st separation data are in agreement, and to attest with said phase hand-loom machine being a just device when in agreement, A 2nd encryption means to encipher said 2nd separation data when said authentication is made, It has a 2nd transmitting means to answer said phase hand-loom machine by using said enciphered 2nd separation data as response data. Said data transfer key generation means By combining said 1st random number and said 2nd separation data, it is encryption equipment according to claim 2 which generates said data transfer key and is characterized by realizing said decryption means, said separation means, and said 2nd encryption means in the circuit in said IC.

[Claim 14] The algorithm of encryption by said transfer data encryption means is encryption equipment according to claim 13 characterized by being the same as that

of at least one thing of said 1st encryption means, said 2nd encryption means, and said decryption means.

[Claim 15] The algorithm of encryption by said transfer data encryption means is encryption equipment according to claim 13 which differs from anything of said 1st encryption means, said 2nd encryption means, and said decryption means, and is characterized by being simpler than which thing.

[Claim 16] Said transfer data encryption means is encryption equipment according to claim 15 characterized by enciphering said transfer data using the part to which said data transfer key corresponds to the block of fixed length to a break and each block.

[Claim 17] Said transfer data encryption means is encryption equipment according to claim 16 characterized by performing said encryption by taking the exclusive OR of said block and part to which said data transfer key corresponds.

[Claim 18] Each of encryption with said 1st encryption means and said 2nd encryption means and decryptions with said decryption means is encryption equipment according to claim 17 characterized by being the same conversion algorithm.

[Claim 19] It is encryption equipment according to claim 18 characterized by for said 1st encryption means, said 2nd encryption means, and said decryption means performing said encryption and decryption using the key data beforehand held in said IC, storing a part of the key data in the mask-ROM field in said IC, and storing the part which remains in the postscript ROM field in said IC.

[Claim 20] It is the communication system which consists of the transmitters and receivers which perform share-izing of a data transfer key, and cryptocommunication using the data transfer key. These transmitters and a receiver A 1st random-number generation means to attest mutually that a phase hand-loom machine is a just device by the communication link based on the Challenge Handshake Authentication Protocol of a challenge response mold, and to generate the 1st random number for challenge data, respectively, A 2nd random-number generation means to generate the 2nd random number for said data transfer keys, and the coupling means which combines said 1st random number and said 2nd random number, An encryption means to encipher said joint data, and a 1st transmitting means to transmit said enciphered joint data to said phase hand-loom machine, A 1st receiving means to receive the enciphered joint data which were transmitted from the 1st transmitting means of said phase hand-loom machine, A separation means to divide a decryption means to decrypt said received joint data, and said decrypted joint data into the 1st separation data equivalent to response data, and the 2nd separation data for said data transfer keys, A 2nd transmitting means to answer said phase hand-loom machine by using said 1st separation data as response data, A 2nd receiving means to receive the 1st separation data answered from the 2nd transmitting means of said phase hand-loom machine, By combining a comparison means to compare with said 1st random number said 1st separation data to which it received, and to attest said phase hand-loom machine with a just device when in agreement, and said 2nd random number and said

2nd separation data Encryption equipment characterized by having a cryptocommunication means to perform said phase hand-loom machine and cryptocommunication using a data transfer key generation means to generate said data transfer key, and said data transfer key generated when said authentication was made.

[Claim 21] It is the communication system which consists of the transmitters and receivers which perform share-izing of a data transfer key, and cryptocommunication using the data transfer key. These transmitters and a receiver A 1st random-number generation means to attest mutually that a phase hand-loom machine is a just device by the communication link based on the Challenge Handshake Authentication Protocol of a challenge response mold, and to generate the 1st random number for challenge data, respectively, A 1st transmitting means to transmit said 1st random number to said phase hand-loom machine, and a 1st receiving means to receive the 1st random number transmitted from the 1st transmitting means of said phase hand-loom machine, A 2nd random-number generation means to generate the 2nd random number for said data transfer keys, and the coupling means which combines said 1st received random number and said 2nd random number, An encryption means to encipher said joint data, and a 2nd transmitting means to answer said phase hand-loom machine in said enciphered joint data, A 2nd receiving means to receive the encryption joint data transmitted from the 2nd transmitting means of said phase hand-loom machine, A separation means to divide a decryption means to decrypt said received joint data, and said decrypted joint data into the 1st separation data equivalent to response data, and the 2nd separation data for said data transfer keys, By combining a comparison means to compare said 1st separation data with said 1st random number generated with said 1st random-number generation means, and to attest said phase hand-loom machine with a just device when in agreement, and said 2nd random number and said 2nd separation data Encryption equipment characterized by having a cryptocommunication means to perform said phase hand-loom machine and cryptocommunication using a data transfer key generation means to generate said data transfer key, and said data transfer key generated when said authentication was made.

[Claim 22] It is the communication system which consists of the transmitters and receivers which perform share-izing of a data transfer key, and cryptocommunication using the data transfer key. These transmitters and a receiver It is what attests mutually that a phase hand-loom machine is a just device by the communication link based on the Challenge Handshake Authentication Protocol of a challenge response mold. Said transmitter It has a 1st random-number generation means to generate the 1st random number, a 1st encryption means to encipher said 1st random number, and a 1st transmitting means to transmit said 1st enciphered random number to a receiver. Said receiver By combining said 1st random number and said 2nd random number with a 1st receiving means to receive said 1st enciphered random number, a

1st decryption means to decrypt said 1st received random number, and a 2nd random-number generation means to generate the 2nd random number The 1st coupling means which generates joint data, and a 2nd encryption means to encipher said joint data, A 2nd receiving means by which have a 2nd transmitting means to transmit said enciphered joint data to a transmitter, and said transmitter receives said enciphered joint data further, A separation means to divide a 2nd decryption means to decrypt said received joint data, and said decrypted joint data into the 1st separation data equivalent to said 1st random number, and the 2nd separation data equivalent to said 2nd random number, A 1st comparison means to compare said 1st random number and said 1st separation data, and to attest said receiver with a just device when in agreement, A 3rd encryption means to encipher said 2nd separation data when said authentication is made, By combining the 1st random number of an account generated with a 3rd transmitting means to transmit said enciphered 2nd separation data to said receiver, and said 1st random-number generation means, and the 2nd separation data obtained with said separation means A 3rd receiving means by which have a 1st data transfer key generation means to generate said data transfer key, and said receiver receives said enciphered 2nd separation data further, A 2nd comparison means to compare a 3rd decryption means to decrypt said received 2nd separation data with said 2nd separation data, with which it was decrypted and said 2nd random number, and to attest said transmitter with a just device when in agreement, By combining said 1st random number obtained with said 1st decryption means, and the 2nd random number generated with said 2nd random-number generation means, when said authentication is made A 4th encryption means by which have a 2nd data transfer key generation means to generate said data transfer key, and said transmitter enciphers transfer data further using the data transfer key generated with said 1st data transfer key generation means, A 4th receiving means by which have a 4th transmitting means to transmit the enciphered transfer data to said receiver, and said receiver receives said enciphered transfer data from said transmitter further, Encryption equipment characterized by having a 4th decryption means to decrypt transfer data using the data transfer key generated with said 2nd data transfer key generation means.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to encryption equipment especially realizable on a scale of a small circuit about the encryption equipment with which the

communication equipment which shares a private key and performs cryptocommunication is equipped.

[0002]

[Description of the Prior Art] The data which are communicating through the channel are unjustly copied on a channel, or there are many cases where it is necessary to prevent being changed. For example, it is a case so that works, such as a film, are digitized, an information compression is carried out further, digital recording is further carried out on the optical disk, this is taken out as electric information with an optical disk regenerative apparatus, it may be elongated by information expanding equipment and the taken-out digital information may be reproduced by the image sound system.

[0003] If this commo data is recorded by the digital information recording apparatus without an author's permission and is further reproduced by digital information duplicate equipment when an optical disk regenerative apparatus and information expanding equipment are separated as a separate device and data communication of the meantime is carried out by the digital communication way, the work of that film will be reproduced unjustly and disturbance of copyright will take place here. Therefore, the data which are communicating through the channel must prevent being unjustly copied on a channel. To generally neither the circuit in a device nor the specification of components being exhibited, since electrical characteristics and the signal format for data communication are generally exhibited in many cases, they become the problem that the alteration of the data which follow the illegal copy of data and it in a channel is big.

[0004] More various things than before are known about the technique for eliminating such a malfeasance and securing a safe communication link. The most typical thing uses a partner authentication technique. Only when this attests fundamentally the justification of the side which the side which sends out data receives and it is able to check that he is a just addressee, it is transmitting data, and a digital work prevents being received by the inaccurate device.

[0005] In addition, the side which checks a partner's justification for the side which proves its justification like the addressee in this case like a testifier, a call, and the transmitting person in this case is called an authentication person. Moreover, in a case like the device in connection with the above-mentioned optical disk record playback, whether these devices are based on the specification defined according to the industry of an optical disk related equipment poses a problem from whether authentication is successful between specific devices. Therefore, in such a case, "justification" means "being based on predetermined specification."

(The 1st conventional technique) As 1st concrete conventional technique, there is the one direction authentication approach using the code technique indicated by the International Standards ISO/IEC 9798-2.

[0006] This authentication approach is based on proving to an authentication person that a testifier has data of the secrecy called an authentication key, without telling

that key itself. Therefore, the data which have an authentication person first are chosen and this is thrown to a testifier. The data which challenged and threw this act are called challenge data. On the other hand, a testifier enciphers said challenge data using the code conversion and the authentication key which were owned beforehand. And the enciphered data are returned to an authentication person. A response is called for this act and response data are called for that data.

[0007] The authentication person who received this response data is sharing the decode conversion and the authentication key which are inverse transformation of the code conversion which the testifier owns, and decrypts the response data answered by the testifier using that authentication key and decode conversion. If this result is in agreement with said challenge data, an addressee will judge it as a thing with the authentication key of normal, and will attest a testifier's justification. One direction authentication means that one side proves the justification on another side.

[0008] Here, the code conversion T is the map to the cipher set from a plaintext set which becomes settled with the key data S . It is a cipher when a plaintext is set to X . It is written as $T(S, X)$. The relation of $TINV(S, T(S, X)) = X$ between the inverse transformation $TINV$ which is the maps to the plaintext set from a cipher set which becomes settled with the same key data S is. It means that it will return if this carries out code conversion of the plaintext X and this is transformed inversely. The inverse transformation of code conversion is called decode conversion. In order to be code conversion, when there is no information of Key S , it is required for it to be difficult to ask for Plaintext X from Cipher $T(S, X)$. In addition, code conversion is described as $E(S,)$, and a practice describes decode conversion $D(S,)$.

[0009] Drawing 11 is drawing showing an example of the authentication approach indicated by said specification. The case where the digital work m_j is transmitted is shown to the 2nd device 12 from the 1st device 11 by drawing 11. Here, the 1st device 11 checks the justification of the 2nd device 12. Actuation of this conventional one direction authentication approach is explained according to the step number shown in this drawing below.

[0010] (1) The 1st device 11 generates a random number $R1$. And it transmits to the 2nd device 12 through a channel by making this into challenge data.

(2) The 2nd device 12 will encipher this random number by making into a cryptographic key the authentication key S of the secrecy stored in the 2nd device 12, if this random number is received. And as a result, it transmits to the 1st device 11 through a channel by using $C1$ as response data.

[0011] (3) The 1st device 11 will decrypt this response data $C1$ by using as a decode key the authentication key S stored in the 1st device 11, if this response data is received.

(4) The 1st device 11 compares $RR1$ with the random number $R1$ stored temporarily in the 1st device 11 as a result of decode. If this is in agreement, the 1st device 11 will think that the 2nd device 12 device holds the same authentication key S , and will

attest with a communications partner being just. On the other hand, if not in agreement, a communications partner judges it as that which is not just, and interrupts processing.

[0012] (5) The 1st device 11 transmits a digital work to the 2nd device 12 through a channel, after attesting the 2nd device 12 with a just thing. When the 3rd device which does not have the authentication key S instead of the 2nd device 12 is connected to the channel Since the 3rd device cannot create the data C1 of a right value at the above-mentioned step (2) and its RR1 does not correspond with said R1 at a step (3) as a result as a result of decode, in a step (4), as for the 1st device 11, a digital work is not transmitted to the 3rd device.

[0013] In addition, if the same challenge data and response data are always used between the 1st device 11 and the 2nd device 12, it is possible that the 3rd inaccurate device which got to know that turns into the 2nd device 12, and it clears up. In order to avoid this, from the 1st device 11, challenge data (random number) different each time are sent.

It is also possible to send out unjustly the data of the falsehood memorized by the hard disk drive unit after authentication with the conventional technique of the above 1st in (the 2nd conventional technique) and time to the 2nd device 12 which has the authentication key of normal, for example. It is necessary to check the justification of the 1st device 11 also for the 2nd device 12 at the same time the 1st device 11 checks the justification of the 2nd device 12, in order to solve this problem.

[0014] Moreover, it is possible to extract the data on this channel to the midst which is transmitting the digital work to the 2nd device 12 through a channel after both devices attest, and to memorize this to it at a hard disk drive unit. Although for that information, such as the electrical characteristics of the signal on a channel and data format, is required, of course, since especially those information is not the information generally made into secrecy, sampling of that digital work is fully technically possible. Therefore, just authentication is inadequate, and after authentication is successful, the new key generated at random is shared between each device, and it is necessary to carry out cryptocommunication which enciphers and transmits a digital work using the key. In addition, the private key for enciphering data which should be transmitted, such as a digital work, is hereafter called a "data transfer key."

[0015] The one direction authentication which is the conventional technique of the above 1st is extended hereafter, and the 2nd conventional technique which performs bidirectional authentication, share-izing of a data transfer key, and cryptocommunication is explained. Drawing 12 shows an example of equipment which realizes this bidirectional authentication. The case where it transmits to drawing 12 after enciphering the digital work nj from the 1st device 21 to the 2nd device 22 is shown.

[0016] This conventional bidirectional authentication and actuation of share-izing of a data transfer key are explained according to the step number shown in this drawing

below.

(1) The 1st device 21 generates a random number R1. This has the semantics as 1st challenge data. And this is transmitted to the 2nd device 22 through a channel. A random number R2 has the semantics as 2nd challenge data from the 2nd device 22 to the 1st device 21 here. That is, a cipher C1 has the semantics of both response data and the 2nd challenge data to the 1st challenge data.

[0017] (2) The 2nd device 22 generates a random number R2, and create joint data $R1||R2$ by combining the random number R1 received from it and the 1st device 21. It is shown that notation " $||$ " puts both data in order in the direction of a digit, and joins together here. And these joint data $R1||R2$ are enciphered by making the authentication key S of the 2nd device 22 into a cryptographic key, and that cipher C1 is transmitted to the 1st device 21.

[0018] (3) The 1st device 21 decrypts the authentication key S for the cipher C1 received from the 2nd device 22 as a decode key, and use the high order of the result as the separation data RR1, and it uses low order as the separation data RR2.

(4) The 1st device 21 compares this separation data RR1 with the random number R1 stored temporarily to the 1st device 21. If this is in agreement, a communications partner will attest with it being a just device with the authentication key S. If not in agreement, authentication processing is interrupted here.

[0019] (5) The 1st device 21 generates a random number K, and sets this up as a data transfer key K. And joint data $RR2||K$ which combined said gained separation data RR2 and this data transfer key K is enciphered with the authentication key S of the 1st device 21, and that cipher C2 is transmitted to the 2nd device 22.

(6) The 2nd device 22 decrypts the cipher C2 received from the 1st device 21 using the authentication key S, and use the high order as the separation data RRR2, and it uses low order as the separation data KK.

[0020] (7) The 2nd device 22 compares this separation data RRR2 with the random number R2 stored temporarily to the 2nd device 22. If this is in agreement, a communications partner will attest with it being a just device with the authentication key S. If not in agreement, authentication processing is interrupted here. On the other hand, decrypted KK separation data is set up as a data transfer key KK.

[0021] (8) The 1st device 21 enciphers a digital work using said data transfer key K, and transmits it to the 2nd device 22 through a channel.

(9) By the 2nd device 22, decrypt this using KK said data transfer key, and gain the digital work of a basis. Here, when the 1st device 21 has the authentication key S of normal and the 2nd device 22 does not have the authentication key of normal, the 1st device 21 is judged to be that in which the communications partner does not have the authentication key of normal at a step (4), and authentication processing can be interrupted. Moreover, the 1st device 21 does not have the authentication key of normal, but when it has the authentication key of normal, in a step (7), the 2nd device 22 judges the 2nd device 22 to be that in which the communications partner does not

have the authentication key of normal, and can interrupt authentication processing. Thus, while a digital work prevents flowing into an inaccurate device, flowing into a just device from an inaccurate device can also be prevented.

[0022] Furthermore, when it has the authentication key also with just 1st device 21 and 2nd device 22, and said authentication processing is completed and the digital work is transmitted in the channel top in the step (8) Since the digital work is enciphered even if it is the case where the digital work was copied electrically and accumulated in digital are recording equipment, it is meaningless digital data and the original digital work is protected effectively.

[0023] As mentioned above, in order to perform bidirectional authentication using a code technique with the sufficient result, it becomes indispensable conditions that what is going to perform injustice does not understand easily the authentication key stored in the interior of the 1st device 21 and the 2nd device 22. Moreover, it is required that neither the generation section of the random number for challenge data nor the generation section of the data transfer key K can access from the exterior and to be unable to change.

[0024] The most effective method of securing the secrecy nature of these components is an approach of realizing as an IC the part which performs the above-mentioned authentication, share-izing of a data transfer key, and cryptocommunication. It is because a great effort is generally applied to analyzing IC, so an authentication key etc. is not decoded easily.

[0025]

[Problem(s) to be Solved by the Invention] However, in order to realize the 1st device 21 in the above-mentioned 2nd conventional technique by IC, such an IC (henceforth "Encryption IC") needs to have the following part.

- Combine the random-number generation section and the separation data RR2 for generating the comparator and the data transfer key K for comparing the part and the random number R1, and the separation data RR1 which store the decode section and the authentication key S for decrypting the random-number generation section and the cipher C1 which generates a random number R1, and the data transfer key K. The hardware of magnitude comparable as this also about the 2nd device 22 of a cryptopart which enciphers a digital work using the part and the data transfer key K which stores the cryptopart and the data transfer key K for enciphering is required.

[0026] thus, having realized the above-mentioned conventional authentication method by IC -- if -- the two random-number generation sections and two converters (the decode section and cryptopart) -- since it must have very many functions, circuit magnitude becomes large and it has the trouble of leading to the cost rise of a device after all. Moreover, it is more desirable for this key to reflect the value which both devices generated for the reason same although the 1st device 21 is generating the data transfer key K for enciphering data with the above-mentioned 2nd conventional technique as mutual recognition being needed.

[0027] As explained above, in order to protect the circuit between devices, the approach of confining the information on functions, such as authentication, or the secrecy for it in IC, and realizing is effective. However, in the conventional approach, by realizing all of the part of mutual recognition, the part of share-izing of a data transfer key, and the part of data encryption by one IC, the magnitude of the IC becomes very large and leads to a cost rise.

[0028] Then, this invention is equipped with the small encryption IC of magnitude, and sets it as the 1st object to offer the encryption equipment which has a necessary minimum function for securing the safety of the communication link between devices. Encryption IC has the following function here.

(1) Store an authentication key in insurance. As for the key, rewriting and read-out are not made by access from the outside.

[0029] (2) Share a data transfer key safely. As for the key, rewriting and read-out are not made by access from the outside.

(3) However, make magnitude of Encryption IC into min by not equipping Encryption IC with the part irrelevant to the safety of communication system. Moreover, the 2nd object of this invention is offering a cryptocommunication system with high safety suitable realizing using the small encryption IC of magnitude.

[0030]

[Means for Solving the Problem] In order to attain the 1st object of the above, this invention is encryption equipment with which the device which performs share-izing of a data transfer key and cryptocommunication which used the data transfer key is equipped. A 1st random-number generation means to generate the 1st random number for share-izing of said data transfer key, A 1st random-number maintenance means to hold the 1st random number generated by said 1st random-number generation means, A 1st transmitting means to transmit the 1st random number generated by said 1st random-number generation means to the phase hand-loom machine of said cryptocommunication, the 1st random number held at said 1st random-number maintenance means — using — the time — said strange data transfer key — generating — data transfer — a key — generation — a means — It has a transfer data encryption means to encipher using said data transfer key to the transfer data set as the object of cryptocommunication. Said 1st random-number generation means, said 1st random-number maintenance means, said data transfer key generation means, and said transfer data encryption means are realized in the circuit in one IC, and said 1st random-number maintenance means is characterized by holding said 1st random number to the field which cannot be accessed from the outside of said IC.

[0031] since the 1st random number relevant to generation of a data transfer key is directly held by this inside [which cannot be accessed from the outside] Encryption IC — the time — a strange data transfer key — each device — insurance — sharing — having — cryptocommunication — carrying out — having . Moreover, since

Encryption IC has a necessary minimum function for securing the safety of the communication link between devices, it is realizable in a small circuit.

[0032] In order to attain the 2nd object of the above moreover, this invention It is the communication system which consists of the transmitters and receivers which perform share-izing of a data transfer key, and cryptocommunication using the data transfer key. These transmitters and a receiver A 1st random-number generation means to attest mutually that a phase hand-loom machine is a just device by the communication link based on the Challenge Handshake Authentication Protocol of a challenge response mold, and to generate the 1st random number for challenge data, respectively, A 2nd random-number generation means to generate the 2nd random number for said data transfer keys, and the coupling means which combines said 1st random number and said 2nd random number, An encryption means to encipher said joint data, and a 1st transmitting means to transmit said enciphered joint data to said phase hand-loom machine, A 1st receiving means to receive the enciphered joint data which were transmitted from the 1st transmitting means of said phase hand-loom machine, A separation means to divide a decryption means to decrypt said received joint data, and said decrypted joint data into the 1st separation data equivalent to response data, and the 2nd separation data for said data transfer keys, A 2nd transmitting means to answer said phase hand-loom machine by using said 1st separation data as response data, A 2nd receiving means to receive the 1st separation data answered from the 2nd transmitting means of said phase hand-loom machine, By combining a comparison means to compare with said 1st random number said 1st separation data to which it received, and to attest said phase hand-loom machine with a just device when in agreement, and said 2nd random number and said 2nd separation data It is characterized by having a cryptocommunication means to perform said phase hand-loom machine and cryptocommunication using a data transfer key generation means to generate said data transfer key, and said data transfer key generated when said authentication was made.

[0033] A cryptocommunication system with high safety is directly realized by two random numbers relevant to not being transmitted and received if the random number relevant to generation of that a data transfer key is generated while mutual recognition is performed between a transmitter and a receiver by this, and a data transfer key remains as it is directly, and generation of a data transfer key suitable to realize using the small encryption IC of magnitude, since it is provided from a transmitter and a receiver, respectively.

[0034]

[Embodiment of the Invention]

(Gestalt 1 of operation) Drawing 1 is drawing showing the processing sequence in the gestalt 1 of the operation which performs mutual recognition, share-izing of a data transfer key, and cryptocommunication of data between the 1st device equipped with the encryption equipment concerning this invention, and the 2nd device.

[0035] The case where the digital work m_j is transmitted is shown to the 2nd device 52 from the 1st device 51 by drawing 1. In addition, only the encryption equipment with which each devices 51 and 52 are equipped is shown in drawing 1, and other components (the transceiver section, processor of a digital work, etc.) irrelevant to encryption equipment and direct are omitted. The encryption equipment concerning this invention with which the 1st device 51 was equipped is roughly divided, and consists of MPU53 and the 1st encryption IC 54.

[0036] MPU53 becomes this encryption equipment from ROM holding the control program of a proper, the general-purpose microprocessor which performs that control program, RAM, etc., and performs processing (the step in drawing (1), (7)) which does not participate in share-ization of a data transfer key directly. The 1st encryption IC 54 is the semiconductor IC of one chip, and performs processing (the step in drawing (3), (5), (9), (11)) which participates in share-ization of a data transfer key directly.

[0037] The encryption equipment which similarly is applied to this invention with which the 2nd device 52 was equipped is also roughly divided, and consists of MPU55 and the 2nd encryption IC 56. MPU55 becomes this encryption equipment from ROM holding the control program of a proper, the general-purpose microprocessor which performs that control program, RAM, etc., and performs processing (the step in drawing (2), (8)) which does not participate in share-ization of a data transfer key directly.

[0038] The 2nd encryption IC 56 is the semiconductor IC of one chip, and performs processing (the step in drawing (4), (6), (10), (12)) which participates in share-ization of a data transfer key directly. In addition, in the gestalt of this operation, 64 bit-block cryptographic algorithm E based on a Data Encryption Standard (DES:Data EncryptionStandard) and its inverse transformation algorithm D are used. Henceforth, "encryption" and the conversion using the inverse transformation algorithm D of the conversion which uses cryptographic algorithm E are called "a decryption."

[0039] Moreover, the 1st encryption IC 54 is equipped only with cryptographic algorithm E, and the 2nd encryption IC 56 is equipped with the inverse transformation algorithm D. This is for reducing the magnitude of each encryption 54 and ICs 56, and safety. Hereafter, according to the step number shown in drawing 1, actuation of the encryption equipment in the gestalt 1 of operation is explained.

[0040] (1) While generating and memorizing a random number R1 (32 bits) in MPU53 of the 1st device 51, pass the 1st encryption IC 54.

(2) Like a step (1), while generating and memorizing a random number R2 (32 bits) in MPU55 of the 2nd device 52, transmit to the 2nd encryption IC 56.

[0041] (3) Store in the field which cannot access a random number R3 (32 bits) from generation and the exterior in the 1st encryption IC 54. And the random number R1 generated by said MPU and said random number R3 are combined, and it enciphers with E function. Here, it is shown that notation "||" combines two random numbers in the direction of a digit, and considers as 64 bits (it is 32 bits of low order about 32

bits of high orders and a random number R3 in a random number R1). Moreover, the authentication key S of the secrecy currently beforehand held in common by the 1st encryption IC 54 and the 2nd encryption IC 56 is used for encryption. The 1st encryption IC 54 transmits the above-mentioned code result C1 to the 2nd device 52 through the transmitting section (not shown by a diagram) of the 1st device 51.

[0042] (4) Like a step (3), in the 2nd encryption IC 56, generate a random number R4 (32 bits), and store in the field which cannot be accessed from the exterior. The random number R2 generated by said MPU and said random number R4 are combined, and it decrypts with the inverse transformation algorithm D. Said authentication key S is used for decode. The 2nd encryption IC 56 transmits the decode result C2 (64 bits) to the 1st device 51 through the transmitting section (not shown by a diagram) of the 2nd device 52.

[0043] (5) Encipher the decode sentence C2 which received from said 2nd device 52 with said authentication key S in the 1st encryption IC 54 using said E function. And obtained 64 bits are divided into the separation data RR2 which are 32 bits of the high order, and the separation data RR4 which are 32 bits of low order. Furthermore, it transmits to the 2nd device 52 through the transmitting section of the 1st device 51, and, on the other hand, the separation data RR2 store the separation data RR4 in the field which cannot be accessed from the outside in the 1st encryption IC 54, without taking out outside.

[0044] In addition, the 1st encryption IC 54 and the 2nd encryption IC 56 are mutually regular, and when the same authentication key S is held, in accordance with the random number R2 which MPU55 of said 2nd device 52 generated, said separation data RR4 of said separation data RR2 correspond with the random number R4 which said 2nd encryption IC 56 stores in the interior.

(6) Decrypt the cipher C1 received from said 1st encryption IC 54 with said authentication key S in the 2nd encryption IC 56 like a step (5) using said inverse transformation algorithm D. And obtained 64 bits are divided into the separation data RR1 which are 32 bits of the high order, and the separation data RR3 which are 32 bits of low order. Furthermore, it transmits to the 1st device 51 through the transmitting section of the 2nd device 52, and, on the other hand, the separation data RR1 store the separation data RR3 in the field which cannot be accessed from the outside in the 2nd encryption IC 56, without taking out outside.

[0045] In addition, the 1st encryption IC 54 and the 2nd encryption IC 56 are mutually regular, and when the same authentication key S is held, in accordance with said random number R1, said separation data RR3 of said separation data RR1 correspond with said random number R3.

(7) Compare the random number R1 memorized at said step (1) in MPU53 of the 1st device 51 with the separation data RR1 received from said 2nd device 52, and when in agreement, attest the 2nd device 52 equipped with the 2nd encryption IC 56 and it with a just device.

[0046] (8) Compare the random number R2 memorized at said step (2) in MPU55 of the 2nd device 52 with the separation data RR2 received from said 2nd device 52 like a step (7), and when in agreement, attest the 1st device 51 equipped with the 1st encryption IC 54 and it with a just device.

(9) Create the data transfer key K in the 1st encryption IC 54 by combining the random number R3 memorized at said step (3), and said separation data RR4. Here, the data transfer key K (64 bits) which makes a random number R3 32 bits of a high order, and makes the separation data RR4 32 bits of low order is generated, in addition -- since this data transfer key K is association of two random numbers -- the time -- queerness, i.e., the key newly generated at random, -- it can say .

[0047] (10) Generate the data transfer key K by combining the random number R4 memorized at said separation data RR3 and said step (4) in the 2nd encryption IC 56 like a step (9). Here, the data transfer key K (64 bits) which makes the random number R4 which memorized the above-mentioned separation data RR3 at 32 bits of a high order and the above-mentioned step (4) 32 bits of low order is generated, this data transfer key -- the time -- a strange key -- it is .

[0048] in addition, when mutual authentication at a step (7) and a step (8) is successful Since the random number R3 generated at the step (3) and the separation data RR3 obtained at the step (6) will be in agreement and the random number R4 generated at the step (4) and the separation data RRR4 obtained at the step (5) will be in agreement consequent -- a step (9) and a step (10) -- the data transfer key K which comes out, respectively and is generated will be in agreement.

[0049] (11) In the 1st encryption IC 54 of the 1st device 51, repeat until it finishes transmitting all the digital works that should transmit the processing which enciphers the blocked digital work mj (64 bits) which is sent from MPU53 using the data transfer key K obtained at the above-mentioned step (9), and transmits the acquired cipher Cj to the 2nd device 52.

[0050] (12) Receive the enciphered above-mentioned digital work Cj (64 bits) which the 1st device 51 transmitted in the 2nd encryption IC 56 of the 2nd device 52 corresponding to a step (11), decrypt using the data transfer key K obtained at the above-mentioned step (10), and send the obtained digital work mmj to MPU55. This decryption is repeated as long as the above-mentioned digital work Cj is transmitted from the 1st device 51.

[0051] Thus, mutual recognition, share-izing of the data transfer key K, and cryptocommunication of data are performed by the encryption equipment of the gestalt 1 of operation between the 1st device 51 and the 2nd device 52. The encryption equipment of the gestalt 1 of the above-mentioned implementation has the following descriptions so that clearly from the above explanation.

[0052] The 1st description is that the data transfer key K is protected by insurance inside Encryption IC. If it is encryption equipment with which the 1st device 51 is equipped, in order to generate the data transfer key K, specifically, two data used

directly, i.e., a random number R3 and the separation data RR4, will fulfill the following conditions.

– The random number R3 is held to the field which it is generated inside the 1st encryption IC 54, and is not outputted outside, and cannot be read from the outside. [0053] – The separation data RR4 are held to the field which it is generated inside the 1st encryption IC 54 (separation generation), and is not outputted outside, and cannot be read from the outside. Since the data transfer key K is protected in Encryption IC by these things, even if it adopts what is exhibited as cryptographic algorithm E and an inverse transformation algorithm D by them, the safety of the cryptocommunication between the 1st device 51 and the 2nd device 52 is guaranteed. [0054] The circuit where the 2nd description is dedicated in Encryption IC is stopped by the necessary minimum thing. If it is encryption equipment with which the 1st device 51 is equipped, specifically, the following processings are realized by the circuit 53 besides the 1st encryption IC 54, i.e., MPU.

– It is considered so that the comparison with generation and the random number R1 of a random number R1, and the separation data RR1, i.e., the circuit magnitude of the 1st encryption IC 54, may not become large superfluously. These two processings are not participating in generation of the data transfer key K directly about authentication of a phase hand-loom machine. Therefore, even if it is going to carry out injustice using these processings being realized out of IC, **** Lycium chinense will be impossible in injustice which brings a profit to the 1st device 51. In addition, creation of the response data RR2 to the challenge data C2 from the 2nd device 52 is performed within Encryption IC.

[0055] Drawing 2 is the block diagram showing the hardware configuration of the 1st encryption IC 54. The 2nd encryption IC 56 is realizable on a scale of comparable hardware. The external I/F section 61 is the only input/output port for accessing the internal circuitry of this 1st encryption IC 54 from the outside. The random-number generation section 60 generates the 32-bit random number R3.

[0056] The random-number storing section 62 is a store circuit holding the random number R3 generated in the random-number generation section 60. A bond part 63 makes the random number R3 stored in the random-number storing section 62 32 bits of low order, and combines the 32-bit data R1 inputted through the external I/F section 61 as 32 bits of high orders.

[0057] The authentication key S storing section 64 is a store circuit holding the authentication key S given beforehand. Switches 65 and 66 are the 3 input 1 output multiplexer of 64-bit width of face, and the 2 input 1 output multiplexer of 64-bit width of face, respectively. The E function 67 is an encryption circuit based on cryptographic algorithm E. A switch 68 is the 1 input 3 output demultiplexer of 64-bit width of face.

[0058] The separation section 69 divides into RR4 64 bit data outputted from the switch 68 32 bit RR2 and 32 bits of low order of high orders. The data transfer key K

generation section 59 makes the random number R3 stored in the random-number storing section 62 32 bits of high orders, is combining the separation data RR4 separated in the separation section 69 as 32 bits of low order, and generates the data transfer key K.

[0059] The data transfer key K storing section 70 is a store circuit holding the data transfer key K generated in the data transfer key K generation section 59. Next, it is shown how it operates in each step each component shown in this drawing 2 was indicated to be to drawing 1 . In the step (3) of drawing 1 , the random-number generation section 60 generates a random number R3, stores it in the random-number storing section 62, and a bond part 63 combines the random number R3 and the random number R1 inputted through the external I/F section 61, and it sends it to the E function 67 through a switch 65. The E function 67 enciphers joint data $R1||R3$ outputted from the bond part 63 using reception and it through the switch 66 in the authentication key S from the authentication key S storing section 64, and, as a result, outputs C1 to the 2nd device 52 through a switch 68 and the external I/F section 61.

[0060] In the step (5) of drawing 1 , and (9), the decode sentence C2 inputted through the external I/F section 61 is inputted into E function through a switch 65. The E function 67 enciphers the decode sentence C2 for the authentication key S storing section 64 to the authentication key S using reception and it, and sends it to the separation section 69 through a switch 68. The separation section 69 divides it into the separation data RR2 and the separation data RR4, and the separation data RR2 are outputted outside through the external I/F section 61, and it sends the separation data RR4 to the data transfer key K generation section 59. After the data transfer key K generation section 59 generates the data transfer key K by combining the random number R3 stored in the random-number storing section 62, and the separation data RR4 sent from the separation section 69, it is stored in the data transfer key K storing section 70.

[0061] In the step (11) of drawing 1 , it enciphers using the data transfer key K in which the digital work mj inputted through the external I/F section 61 and a switch 65 was stored by the data transfer key K storing section 70, and, as a result, the E function 67 outputs Cj to the 2nd device 52 through a switch 68 and the external I/F section 61. In addition, with the gestalt 1 of operation, although concrete bit length and data configurations, such as a random number and a cipher, were shown, this invention is not limited to them. For example, in the above-mentioned step (5), the 32-bit random numbers R1 and R2 are combined, it considers as 64 bits, this is inputted into the 64-bit code function E, and the 64-bit cipher C1 is searched for. This part is good also as a method which generates the 128-bit cipher C1 by making for example, each random number into 64 bits, and repeating encryption by the code function E twice. However, it is required for the part about a random number R1 and the part about R2 to be easily unseparable from a cipher C1 in this case. There is the approach of the code accompanied by a chain like the CBC mode as one of the

approach of the. About the CBC mode, it is detailed to p70 in Shin-ichi Ikeno and Kenji Koyama collaboration "present age code theoretical" IECE 1986.

[0062] moreover — although hardware magnitude is reduced with the gestalt 1 of operation when the 1st encryption IC 54 is equipped with the code function E and the 2nd encryption IC 56 is equipped with the inverse function D — that — the very thing is not the essence of this invention, as mentioned above. That is, it is a matter to determine in relation with the circuit magnitude permitted by these encryption 54 and ICs 56, the class of encryption algorithm, etc., for example, each may own both cryptographic algorithm E and the inverse transformation algorithm D, and the inverse transformation algorithm D may be used for the informational decode to which cryptographic algorithm E was sent by encryption of a random number from the phase hand-loom machine. This invention is because the description is in the point of having secured the safety of secret communication by IC-izing the component in connection with generation of the data transfer key K directly at least.

[0063] Moreover, in the gestalt 1 of operation, the random number R1 in a step (1) may be generated within the 1st encryption IC 54. By this, possibility of using the 1st encryption IC 54 as a decryptor can be abolished, and it can consider as safer encryption equipment. That is, with the gestalt 1 of operation, a random number R1 is generated in the exterior of the 1st encryption IC 54, and the 1st encryption IC 54 outputs a cipher C1 based on this random number R1. Although this cipher C1 is influenced of the random number R3 generated inside the 1st encryption IC 54, when a random number R3 is not a value random enough, it will become possible to abuse the 1st encryption IC 54 as a decryptor. Therefore, by generating a random number R1 within the 1st encryption IC 54, the possibility of the attack described above disappears and this encryption equipment will become safer.

(Gestalt 2 of operation) Next, the gestalt 2 of operation is shown as a modification of the step in the gestalt 1 of operation shown in drawing 1 . The object and effectiveness are the same as the gestalt 1 of operation. Moreover, it is comparable as the gestalt 1 of operation shown in drawing 2 also as hardware magnitude. With the gestalt 1 of operation, response data were enciphered and it communicated without enciphering challenge data, but with the gestalt 2 of operation, it communicates without enciphering challenge data and enciphering response data. It explains focusing on the point which is different from the gestalt 1 of operation.

[0064] Drawing 3 is drawing showing the processing sequence in the gestalt 2 of the operation which performs mutual recognition, share-izing of a data transfer key, and cryptocommunication of data between the 1st device 71 equipped with the encryption equipment concerning this invention, and the 2nd device 72. The case where the digital work mj is transmitted is shown to the 2nd device 72 from the 1st device 71 by drawing 3 .

[0065] MPU73, the 1st encryption IC74 and MPU75, and the 2nd encryption IC 76 correspond to MPU53 in the gestalt 1 of operation, the 1st encryption IC54 and

MPU55, and the 2nd encryption IC 56, and are the same as that of the case of the gestalt 1 of operation about a hardware configuration except for a difference of procedure. Hereafter, according to the step number shown in drawing 3, actuation of the encryption equipment in the gestalt 2 of operation is explained.

[0066] (1) While generating and memorizing a random number R1 (32 bits) in MPU73 of the 1st device 71, transmit to the 2nd device 72 through the transmitting section (not shown by a diagram) of the 1st device 71. This is passed to the 2nd encryption IC 76 by the 2nd device 72.

(2) Like a step (1), while generating and memorizing a random number R2 (32 bits) in MPU75 of the 2nd device 72, transmit to the 1st device 71 through the transmitting section (not shown by a diagram) of the 2nd device 72. This is passed to the 1st encryption IC 74 by the 1st device 71.

[0067] (3) In the 1st encryption IC 74, generate a random number R3 (32 bits), and store in the field which cannot be accessed from the exterior. The random number R2 received from said 2nd device 72 and said random number R3 are combined, and it enciphers with E function. The authentication key S of the secrecy currently beforehand held in common by the 1st encryption IC 74 and the 2nd encryption IC 76 is used for encryption. The 1st encryption IC 74 transmits the encryption result C1 (64 bits) to the 2nd device 72.

[0068] (4) Like a step (3), in the 2nd encryption IC 76, generate a random number R4 (32 bits), and store in the field which cannot be accessed from the exterior. The random number R1 received from said 1st device 71 and said random number R4 are combined, and it decrypts with the inverse transformation algorithm D. Said authentication key S is used for decode. The 2nd encryption IC 76 transmits the decode result C2 (64 bits) to the 1st device 71.

[0069] (5) Encipher the decode sentence C2 which received from said 2nd encryption IC 76 with said authentication key S in the 1st encryption IC 74 using said E function. Among 64 bit data of the result, let 32 bits of high orders as the separation data RR1, and let 32 bits of low order be the separation data RR4. And the separation data RR1 store in MPU73 of the 1st device 71 to delivery and the field which cannot be accessed from the outside in the 1st encryption IC 74 on the other hand, without taking out the separation data RR4 outside.

[0070] In addition, the 1st and 2nd encryption IC 76 is mutually regular, when the same authentication key S is held, said separation data RR1 become the same as the random number R1 which MPU73 of said 1st device 71 generated, and said separation data RR4 become the same as the random number R4 which the 2nd encryption IC 76 generated.

(6) Decrypt the cipher C1 received from said 1st encryption IC 74 with said authentication key S in the 2nd encryption IC 76 like a step (6) using said inverse transformation algorithm D. Let 32 bits of high orders of 64 bit data of the result as the separation data RR2, and let 32 bits of low order be the separation data RR3. And

the separation data RR2 store in MPU75 of the 2nd device 72 to delivery and the field which cannot be accessed from the outside in the 2nd encryption IC 76 on the other hand, without taking out the separation data RR3 outside.

[0071] In addition, the 1st and 2nd encryption IC 76 is mutually regular, when the same authentication key S is held, said separation data RR2 become the same as the random number R2 which MPU75 of said 2nd device 72 generated, and said separation data RR3 become the same as the random number R3 which the 1st encryption IC 74 generated.

(7) When the separation data RR1 received from said R1 memorized and 1st [said] encryption IC 74 in MPU73 of the 1st device 71 are compared and it is in agreement, attest the 2nd device 72 by which the 2nd encryption IC 76 and the 2nd encryption IC 76 were included with a just device.

[0072] (8) When the separation data RR2 received from said R2 memorized and 2nd [said] encryption IC 76 in MPU75 of the 2nd device 72 are compared like a step (8) and it is in agreement, attest the 1st device 71 by which the 1st encryption IC 74 and the 1st encryption IC 74 were included with a just device.

(9) Create the data transfer key K using said random number R3 and said separation data RR4 within the 1st encryption IC 74. By a diagram, both association is used as the data transfer key K (64 bits).

[0073] (10) Create the data transfer key K like the 1st encryption IC 74 like a step (10) using said separation data RR3 and said random number R4 within the 2nd encryption IC 76. By a diagram, both association is used as the data transfer key K (64 bits).

(11) In the 1st encryption IC 74 of the 1st device 71, repeat until it finishes transmitting all the digital works that should transmit the processing which enciphers the blocked digital work mj (64 bits) which is sent from MPU73 using the data transfer key K obtained at the above-mentioned step (9), and transmits the acquired cipher Cj to the 2nd device 72.

[0074] (12) Receive the enciphered above-mentioned digital work Cj (64 bits) which the 1st device 71 transmitted in the 2nd encryption IC 76 of the 2nd device 72 corresponding to a step (11), decrypt using the data transfer key K obtained at the above-mentioned step (10), and send the obtained digital work mmj to MPU75. This decryption is repeated as long as the above-mentioned digital work Cj is transmitted from the 1st device 71.

[0075] Thus, mutual recognition, share-izing of the data transfer key K, and cryptocommunication of data are performed by the encryption equipment of the gestalt 2 of operation between the 1st device 71 and the 2nd device 72 like the case of the gestalt 1 of operation. In addition, as mentioned above, the encryption equipment of the gestalt of this operation and the thing of the gestalt 1 of operation are in agreement in a hardware configuration, and procedure, i.e., connection of each hardware configuration element, only differs from an execution sequence. Therefore,

about the description and its modification of the encryption equipment of this operation gestalt, it can say that it is the same as that of the case of the gestalt 1 of operation.

(Gestalt 3 of operation) There are the following common features in the encryption equipment of the gestalten 1 and 2 of the above operation.

(1) In both devices, two random numbers are generated, respectively, one of these is used for authentication, and other one side is used for generation of the data transfer key K.

(2) The random number used for generation of the data transfer key K is not outputted to the exterior of Encryption IC in a form as it is, and, on the other hand, the random number used for authentication is outputted and opened to the exterior of Encryption IC.

[0076] On the other hand, the encryption equipment of the gestalt 3 of operation explained below generates only one random number, and uses it for the object of both the object for authentication, and for generation of a data transfer key. This is for mitigating the burden of random-number generation within Encryption IC compared with the gestalten 1 and 2 of operation. Moreover, in the interior of Encryption IC, the random-number generation and comparison processing for authentication are performed. That is, it is different from the gestalten 1 and 2 of operation, and carries out by the internal circuitry of Encryption IC not only including generation of a data transfer key but including authentication processing. As mentioned above, this is for coping with improper use of using for decryption of Encryption IC, and can raise the safety of cryptocommunication.

[0077] Drawing 4 is drawing showing the processing sequence in the gestalt 3 of the operation which performs mutual recognition, share-izing of a data transfer key, and cryptocommunication of data between the 1st device 71 equipped with the encryption equipment concerning this invention, and the 2nd device 72. The case where the digital work mj is transmitted is shown to the 2nd device 82 from the 1st device 81 by drawing 4.

[0078] In addition, also in the gestalt of this operation, the encryption equipment applied to this invention with which each devices 81 and 82 were equipped like the gestalten 1 and 2 of operation is roughly divided, and consists of MPU 83 and 85 and encryption 84 and ICs 86. However, since MPU 83 and 85 achieves only the function to pass the digital work mj to encryption 84 and ICs 86, it can be said that the encryption equipment concerning this invention consists of encryption 84 and ICs 86 substantially.

[0079] The 1st encryption IC 84 and the 2nd encryption IC 86 are the semiconductor ICs of one chip like the gestalten 1 and 2 of a fruit. Hereafter, according to the step number shown in drawing 4, actuation of the encryption equipment in the gestalt 3 of operation is explained.

(1) While generating and memorizing a random number R1 in the 1st encryption IC 84,

encipher this with E function and transmit a cipher C1 to the 2nd device 82 through the transmitting section (not shown by a diagram) of the 1st device 81. The 2nd encryption IC 86 and the authentication key S of the secrecy currently held in common beforehand are used for encryption. The received cipher C1 is passed to the 2nd encryption IC 86 by the 2nd device 82.

[0080] (2) In the 2nd encryption IC 86, decrypt the received cipher C1 with the inverse transformation algorithm D, and obtain the decode sentence RR1. When the 1st encryption IC 84 and the 2nd encryption IC 86 are the things of normal, this decode sentence RR1 is in agreement with said random number R1.

(3) While generating and memorizing a random number R2 in the 2nd encryption IC 86, combine this with said decode sentence RR1, and decrypt with said inverse transformation algorithm D. Said authentication key S is used for decode. The 2nd encryption IC 86 transmits the decode sentence C2 to the 1st device 81 through the transmitting section (not shown by a diagram) of the 2nd device 82. This is passed to the 1st encryption IC 84 by the 1st device 81.

[0081] (4) In the 1st encryption IC 84, encipher said decode sentence C2 with said E function, and divide the result into the separation data RRR1 and the separation data RR2. In addition, if the separation data RRR1 are the case of an exchange by the just device, they are in agreement with said decode sentence RR1 and random number R1. Moreover, the separation data RR2 are in agreement with said random number R2.

(5) The random number R1 memorized at said step (1) in the 1st encryption IC 84 is compared with said separation data RRR1, and in being in agreement, it attests the justification of the 2nd device 82 including the 2nd encryption IC 86 and the 2nd encryption IC 86.

[0082] (6) In the 1st encryption IC 84, encipher said separation data RR2 with said E function, and transmit to the 2nd device 82. The 2nd device 82 passes this cipher C3 to the 2nd encryption IC 86.

(7) In the 2nd encryption IC 86, decrypt said cipher C3 with said inverse transformation algorithm D, and obtain the decode sentence RRR2.

[0083] (8) In the 2nd encryption IC 86, compare with said decode sentence RRR2 the random number R2 memorized at said step (3), and when in agreement, attest the justification of the 1st device 81 including the 1st encryption IC 84 and the 1st encryption IC 84.

(9) Generate the data transfer key K in the 1st encryption IC 84 by combining said random number R1 and said separation data RR2.

[0084] (10) Generate the data transfer key K in the 2nd encryption IC 86 using said decode sentence RR1 and said random number R2.

(11) In the 1st encryption IC 84 of the 1st device 81, repeat until it finishes transmitting all the digital works that should transmit the processing which enciphers the blocked digital work mj (64 bits) which is sent from MPU83 using the data transfer key K obtained at the above-mentioned step (9), and transmits the acquired cipher Cj

to the 2nd device 82.

[0085] (12) Receive the enciphered above-mentioned digital work Cj (64 bits) which the 1st device 81 transmitted in the 2nd encryption IC 86 of the 2nd device 82 corresponding to a step (11), decrypt using the data transfer key K obtained at the above-mentioned step (10), and send the obtained digital work mmj to MPU85. This decryption is repeated as long as the above-mentioned digital work Cj is transmitted from the 1st device 81.

[0086] Thus, mutual recognition, share-izing of the data transfer key K, and cryptocommunication of data are performed by the encryption equipment of the gestalt 3 of operation between the 1st device 71 and the 2nd device 72 like the case of the gestalten 1 and 2 of operation. In addition, in the above-mentioned step (1), (2), (6), and (7), association of two random numbers is enciphered in encryption of one random number, a step (3), and (4). When using E function of 64-bit width of face, and the inverse transformation algorithm D, it is good to pad the value of 32 bits of immobilization to the 32-bit remaining input about the former, using each random number as 32 bits. For example, it is making a random number into low order 32 BITSU, and making 32 bits of high orders into zero altogether fixed etc. Moreover, about the latter, it is good to input united 64 bits into each function as they are.

[0087] Moreover, when making bit length of each random number into double 64 bits, the former should just perform the code which inputs into a function as it is, repeats each function twice, and uses it about the latter, for example, has a chain like the CBC mode. In the gestalt 3 of the operation described above, it differs in the gestalten 1 and 2 of operation, and the random number for authentication and the random number for share-izing of a data transfer key are made to serve a double purpose. And comparison processing for the random-number generation for authentication or authentication is performed within Encryption IC. Therefore, since a random number does not appear besides Encryption IC if it remains as it is, it is more safe to an attack using Encryption IC as a decoder. Moreover, the number of bits of each random number can secure safety sufficient at least by this.

(Gestalt 4 of operation) Next, the encryption equipment concerning the gestalt 4 of operation is explained.

[0088] This equipment is the operation gestalt which pursued miniaturization of Encryption IC, and is different from the gestalten 1-3 of the above-mentioned implementation in the point which has adopted one direction authentication, and the point that a data transfer key is exhibited. However, cryptographic algorithm E and its inverse transformation algorithm D are premised on being made secrecy. Drawing 5 is drawing showing the processing sequence in the case of transmitting the digital work mj to the 2nd device 92 from the 1st device 91.

[0089] Drawing 6 is the block diagram showing the hardware configuration of the 1st encryption IC 94.

(1) First, the random-number generation section 101 of the 1st encryption IC 94

transmits to the 2nd device 92 through the external I/F section 100 while it generates the random number R1 combining and [challenge] and a data transfer key and stores it in the random-number storing section 102.

(2) To the received random number R1, decrypt the 2nd encryption IC 96 using the 1st encryption IC 94 and the authentication key S owned in common beforehand, and it transmits the obtained decode sentence C1 to the 1st device 91.

[0090] (3) Encipher the E function 106 in the 1st encryption IC 94 using the same thing as the above-mentioned authentication key S beforehand stored in the authentication key S storing section 103 to the decode sentence C1 which received through the external I/F section 100 and a switch 105. The data RR1 obtained as a result are sent to a comparator 108 through a switch 107, and are compared with the random number R1 currently held at the random-number storing section 102 here.

[0091] (4) Since it can attest with the 2nd device 92 being a just device when in agreement as a result, a comparator 108 controls a switch 104 so that the random number R1 currently held at the random-number storing section 102 is used as a data transfer key.

(5) Encipher using the random number R1 sent through a switch 104 to the digital work mj sent through the external I/F section 100 and a switch 105 from MPU93, and transmit the E function 106 to the 2nd device 92 through a switch 107 and the external I/F section 100.

[0092] (6) In the 2nd encryption IC 96 of the 2nd device 92, to the digital work Cj sent from the 1st device 91, decrypt using the random number R1 received at the above-mentioned step (2) as a data transfer key, and send the obtained digital work mmj to MPU95. Thus, with the gestalt of this operation, authentication, share-izing of a data transfer key, and cryptocommunication are realized by the steps and components of the gestalten 1-3 of operation fewer than a case.

[0093] In addition, since the random number R1 transmitted to the 2nd device 92 from the 1st device 91 is used as a data transfer key as it is, a data transfer key may be easily known for the gestalt of this operation by the 3rd person. However, since cryptographic algorithm E and its inverse transformation algorithm D are made into secrecy as mentioned above even if the 3rd person who got to know the data transfer key is going to intercept and decrypt the digital work Cj, the attempt is not successful.

[0094] Moreover, since a means only for the random-number generation section 101 to be able to store the new random number R1 in the random-number storing section 102, and to store the new random number R1 in the random-number generation section 101 from the outside of this 1st encryption IC 94 does not exist even if that 3rd person is going to decode cryptographic algorithm by forging the convenient random number R1, that attempt is not successful, either. Thus, if cryptographic algorithm and its inverse transformation algorithm are made into secrecy, authentication, generation of a data transfer key, and cryptocommunication are realizable with compact encryption IC like the gestalt of this operation.

[0095] In addition, in the gestalten 1-4 of the above-mentioned implementation, the following is desirable as an approach (it is made to memorize) of setting the authentication key S as Encryption IC. That is, some authentication keys S are beforehand set up at the time of manufacture of Encryption IC, and the part which remains is the approach of writing in after manufacture of the encryption IC. A part of authentication key S storing section 64 is constituted from a mask ROM which wrote in some authentication keys S beforehand, and, specifically, the part which remains consists of postscripts ROM which can be written in programmably.

[0096] When constituted only from a mask ROM, this Since through a help for creation of the final encryption IC, while it is safe When there is a fault that the analysis of the set point is easy, in the chip analysis by reverse engineering and it constitutes from postscript ROM on the other hand Since a help is minded and there is a fault that a mistake mixes or injustice becomes possible while the analysis by the reverse engineering of the set point is difficult, it is for compensating both fault of them.

[0097] Moreover, it may be as follows as an example of the cryptographic algorithm in the cryptocommunication of the gestalten 1-4 of the above-mentioned implementation. A digital work is divided into a 64-bit block by the transmitting side, and said data transfer key K (64 bits) and exclusive OR for every bit are taken. The result is made into a cipher. A receiving side should just take similarly the exclusive OR of the 64-bit cipher and the data transfer key K which were received. The block of a basis decodes by this.

[0098] Moreover, the data transfer key K is not considered as immobilization, but there is also the approach of updating the data transfer key K used, while taking a synchronization by the transmitting side and the receiving side for these the blocks of every. For the updating, said E function and inverse transformation algorithm D may be used. The code/decode within a block may be the exclusive ORs described previously. Moreover, although it sets in the gestalten 1-4 of the above-mentioned implementation and some examples of a challenge response mold are shown as the authentication approach, this invention is not restricted to these examples. For example, you may be another example of the challenge response mold of generating a random number by the encryption IC by the side of authentication, sending this as challenge data, and comparing the response data for reference which are an authentication side with the response data returned from the certification side, and were generated.

[0099] in addition -- although the technique of carrying out authentication and cryptocommunication to insurance on a scale of a small circuit was indicated in the gestalten 1-4 of the above-mentioned implementation -- the reinforcement of safety -- therefore, it cannot be overemphasized that required circuit magnitude has the relation of a trade-off. Therefore, the safety of cryptocommunication can be strengthened with carrying out additional installation of a new conversion means to

perform data-conversion $F()$ for the following objects when allowances are in the circuit magnitude which can be mounted in MPU or Encryption IC.

(1) One of them is making a transmission line neither the challenge data of a plaintext nor the response data of a plaintext flow.

[0100] For example, in the processing sequence (a step (1), (3), (6), (7)) with which the 1st device 51 shown in drawing 1 attests the 2nd device 52, it changes as follows. In a step (6), the 2nd encryption IC 56 does not send the separation data RR1 to MPU53, but gives predetermined conversion $F()$ to the separation data RR1, and sends the data $F(RR1)$ obtained as a result to MPU53.

[0101] In a step (7), MPU53 does not compare a random number R1 with the separation data RR1, but gives the same conversion $F()$ as what was used for the random number R1 at the above-mentioned step (6), and compares the data $F(R1)$ obtained as a result with the data $F(RR1)$ sent from the 2nd encryption IC 56. Since it is avoided that a part of cipher C1 and its plaintext RR1 flow a transmission line, the safety to a known plaintext attack is strengthened with doing in this way.

(2) Another is making it not use challenge data as a data transfer key as it is.

[0102] For example, in the step (5) shown in drawing 5, the 1st encryption IC 94 gives predetermined conversion $F()$ to a random number R1, not using a random number R1 as a data transfer key as it is, and uses the data $F(R1)$ obtained as a result as a data transfer key. Similarly, in a step (6), the 2nd encryption IC 96 gives the same conversion $F()$ as what was used for the random number R1 at the above-mentioned step (5), not using a random number R1 as a data transfer key as it is, and uses the data $F(R1)$ obtained as a result as a data transfer key.

[0103] The data transfer key $F(R1)$ can be kept secret, and the safety of cryptocommunication is strengthened with doing in this way.

(3) Another is complicating joint processing further. For example, in the step (9) shown in drawing 1, the 1st encryption IC 54 gives these [R3 and RR4] predetermined conversion $F()$ rather than only combines a random number R3 and the separation data RR4 in the direction of a digit, and uses as the data transfer key K the data $F(R3, RR4)$ obtained as a result.

[0104] Similarly, in a step (10), the 2nd encryption IC 56 does not only combine a random number R4 and the separation data RR3 in the direction of a digit, but gives the same conversion $F()$ as what was used for these [R4 and RR3] at the above-mentioned step (9), and uses as the data transfer key K the data $F(R3, RR4)$ obtained as a result. The generation procedure of the data transfer key K is complicated, and the safety of cryptocommunication is strengthened with doing in this way.

(Example of adaptation to concrete communication system) As mentioned above, the encryption equipment concerning this invention is equipped with the small encryption IC of magnitude, and has a necessary minimum function for securing the safety of the communication link between devices. Therefore, this encryption equipment is suitable

equipment for the communication equipment with which secret communication is needed and a small thing is demanded, for example, the multimedia related equipment treating a portable telephone or a digital work etc.

[0105] Drawing 7 is drawing showing the example of application to the concrete communication system of the encryption equipment concerning this invention, and shows a general view of the regeneration system of digital works, such as a film. This system consists of SCSI cable 116 grade which connects the optical disk drive equipment 110 corresponding to the 1st device in the above-mentioned operation gestalt, the picture reproducer 111 corresponding to the 2nd device, and them. It is the system which enciphers the compression image data read with optical disk drive equipment 110, transmits to picture reproducer 111, and carries out image reproduction there.

[0106] Drawing 8 is the block diagram showing the configuration of optical disk drive equipment 110. MPU124 by which optical disk drive equipment 110 controls the whole equipment, The SCSI controller 121 which is a communication interface with picture reproducer 111, The read-out control section 122 which controls the optical head 125, and reads and controls image data from an optical disk 115, It consists of encryption IC 123 equivalent to the encryption IC of the 1st device in the above-mentioned operation gestalten 1-4. After picture reproducer 111 attests that it is a just device, the image data recorded on the optical disk 115 are read, and it enciphers in encryption IC 123, and transmits to picture reproducer 111 through the SCSI cable 116.

[0107] Drawing 9 is drawing showing a general view of the circuit board mounted in the interior of optical disk drive equipment 110. Encryption IC 123 is LSI formed in one silicon substrate, and is carrying out the configuration of the flat package by which the mould was carried out with plastics. Drawing 10 is the block diagram showing the configuration of picture reproducer 111. MPU131 by which picture reproducer 111 controls the whole equipment, and the SCSI controller 130 which is a communication interface with optical disk drive equipment 110, The encryption IC 132 equivalent to the encryption IC of the 2nd device of the above-mentioned operation gestalten 1-4 It consists of an MPEG decoder 133 which elongates the compression image data decoded by encryption IC 132, and the AV signal-processing section 134 which changes the elongated image data into an analog video signal, and carries out a video output to CRT112 and a loudspeaker 114.

[0108] The digital work recorded on the optical disk 115 by applying the encryption equipment concerning this invention to such an image regeneration system is protected from an illegal copy etc., and the healthy development in the secondary market of a multimedia related product can be expected.

[0109]

[Effect of the Invention] The encryption equipment concerning this invention so that clearly from the above explanation A 1st random-number generation means to be

encryption equipment with which the device which performs share-izing of a data transfer key and cryptocommunication using the data transfer key is equipped, and to generate the 1st random number for share-izing of said data transfer key, A 1st random-number maintenance means to hold the 1st random number generated by said 1st random-number generation means, A 1st transmitting means to transmit the 1st random number generated by said 1st random-number generation means to the phase hand-loom machine of said cryptocommunication, the 1st random number held at said 1st random-number maintenance means -- using -- the time -- said strange data transfer key -- generating -- data transfer -- a key -- generation -- a means -- It has a transfer data encryption means to encipher using said data transfer key to the transfer data set as the object of cryptocommunication. Said 1st random-number generation means, said 1st random-number maintenance means, said data transfer key generation means, and said transfer data encryption means are realized in the circuit in one IC, and said 1st random-number maintenance means is characterized by holding said 1st random number to the field which cannot be accessed from the outside of said IC.

[0110] since the 1st random number relevant to generation of a data transfer key is directly held by this inside [which cannot be accessed from the outside] Encryption IC -- the time -- a strange data transfer key -- each device -- insurance -- sharing -- having -- cryptocommunication -- carrying out -- having . Moreover, since Encryption IC has a necessary minimum function for securing the safety of the communication link between devices, it is realizable in a small circuit.

[0111] Here, said encryption equipment is equipped with a 1st encryption means to encipher further the 1st random number generated by said 1st random-number generation means, said 1st encryption means is realized in the circuit in said IC, and said 1st transmitting means can also be supposed that the 1st random number enciphered with said 1st encryption means is transmitted to said phase hand-loom machine. Thereby, since it becomes impossible for the 3rd person to know the 1st random number relevant to generation of a data transfer key directly, the secrecy nature of a data transfer key is maintained, and cryptocommunication will be maintained even if cryptographic algorithm and its inverse transformation algorithm are known.

[0112] Said device is what said phase hand-loom machine attests mutually that it is a just device with by the communication link based on the Challenge Handshake Authentication Protocol of a challenge response mold here. A 2nd random-number generation means by which said encryption equipment generates further the 2nd random number for challenge data transmitted to said phase hand-loom machine, It judges whether the response data answered from said phase hand-loom machine to said challenge data and said 2nd random number are in agreement. When in agreement, it has an authentication means to attest with said phase hand-loom machine being a just device, and said data transfer key generation means can also be supposed that

said data transfer key is generated when said authentication is made.

[0113] By this, when the mutual recognition between devices is successful, the data transfer key of normal will be generated simultaneously, and the safety of secret communication improves. Here, it can also be supposed that said 2nd random-number generation means and said authentication means are realized in the circuit besides said IC. Thereby, directly, since the processing section irrelevant to generation of the part irrelevant to the safety of communication system, i.e., a data transfer key, is prepared out of Encryption IC, it is controlled that the magnitude of Encryption IC becomes large unnecessarily.

[0114] A decryption means by which said encryption equipment decrypts the enciphered joint data which have been sent from said phase hand-loom machine further here, A separation means to divide the decrypted joint data into the 1st separation data equivalent to response data, and the 2nd separation data which remain, It has a 2nd transmitting means to answer said phase hand-loom machine in said 1st separation data. Said 1st encryption means Said 1st random number and said 2nd random number are combined, and the joint data obtained as a result are enciphered. Said data transfer key generation means By combining said 1st random number and said 2nd separation data, said data transfer key can be generated and it can also be supposed that said decryption means and said separation means are realized in the circuit in said IC.

[0115] Moreover, a 2nd transmitting means for said encryption equipment to use said 2nd random number as challenge data further, and to transmit to said phase hand-loom machine, A decryption means to decrypt the enciphered joint data which have been sent from said phase hand-loom machine, It has a separation means to divide the decrypted joint data into the 1st separation data equivalent to response data, and the 2nd separation data which remain. Said authentication means Said decision and authentication are carried out as response data answered from said phase hand-loom machine in said 1st separation data. Said 1st encryption means The challenge data transmitted from said phase hand-loom machine and said 1st random number are combined, and the joint data obtained as a result are enciphered. Said data transfer key generation means By combining said 1st random number and said 2nd separation data, said data transfer key can be generated and it can also be supposed that said decryption means and said separation means are realized in the circuit in said IC.

[0116] This has a necessary minimum function for securing the safety of the communication link between devices, and encryption equipment equipped with the small encryption IC of magnitude is realized. Here, it can also be supposed that the algorithm of encryption by said transfer data encryption means is characterized by being the same as that of at least one thing of said 1st encryption means and said decryption means.

[0117] Since this becomes possible to make serve a double purpose and mount a transfer data encryption means, the 1st encryption means, and a decryption means by

one converter, the circuit magnitude of Encryption IC is reduced. Here, the algorithm of encryption by said transfer data encryption means differs from anything of said 1st encryption means and said decryption means, and can also be simplified rather than which thing.

[0118] Thereby, since the size of transfer data is large, even if it is a case so that the encryption may be repeated repeatedly, the nonconformity that a data transfer time will benefit encryption long substantially is avoided. Here, said transfer data encryption means can also presuppose that said transfer data are enciphered using a break and the part to which said data transfer key corresponds to each block to the block of fixed length.

[0119] This becomes possible also to the cryptocommunication of the large transfer data of data size to apply this encryption equipment. Here, said transfer data encryption means can also be supposed that said encryption is performed by taking the exclusive OR of said block and part to which said data transfer key corresponds.

[0120] It enables this to realize a transfer data encryption means in a simple logical circuit. Here, also suppose that the code in said 1st encryption means and a decryption with said decryption means are the same conversion algorithms. This becomes possible to make serve a double purpose and mount the 1st encryption means and a decryption means by one converter, and the circuit magnitude of Encryption IC is reduced.

[0121] Here, said 1st encryption means and said decryption means perform said encryption and decryption using the key data beforehand held in said IC, a part of the key data is stored in the mask-ROM field in said IC, and it can also be supposed that the part which remains is stored in the postscript ROM field in said IC. It enables this to compensate an authentication key with the fault at the time of constituting only from a mask ROM, and the fault at the time of constituting from postscript ROM.

[0122] Said device is what said phase hand-loom machine attests mutually that it is a just device with by the communication link based on the Challenge Handshake Authentication Protocol of a challenge response mold here. A decryption means by which said encryption equipment decrypts the enciphered joint data which have been sent from said phase hand-loom machine to said challenge data further, A separation means to divide the decrypted joint data into the 1st separation data equivalent to response data, and the 2nd separation data which remain, An authentication means to judge whether said 1st random number and said 1st separation data are in agreement, and to attest with said phase hand-loom machine being a just device when in agreement, A 2nd encryption means to encipher said 2nd separation data when said authentication is made, It has a 2nd transmitting means to answer said phase hand-loom machine by using said enciphered 2nd separation data as response data. Said data transfer key generation means By combining said 1st random number and said 2nd separation data, said data transfer key can be generated and it can also be supposed that said decryption means, said separation means, and said 2nd encryption

means are realized in the circuit in said IC.

[0123] Since only one random number is generated and it is used for the object of both the object for authentication, and for generation of a data transfer key by this, the circuit magnitude for random-number generation with encryption equipment is mitigated. Moreover, since the random-number generation and comparison processing for authentication are performed in the interior of Encryption IC, the safety of cryptocommunication is raised.

[0124] Moreover, this invention is communication system which consists of the transmitters and receivers which perform share-izing of a data transfer key, and cryptocommunication which used the data transfer key, and can also be supposed that these transmitters and a receiver are equipped with the above-mentioned configuration, respectively. A cryptocommunication system with high safety is directly realized by two random numbers relevant to not being transmitted and received if the random number relevant to generation of that a data transfer key is generated while mutual recognition is performed between a transmitter and a receiver by this, and a data transfer key remains as it is directly, and generation of a data transfer key suitable to realize using the small encryption IC of magnitude, since it is provided from a transmitter and a receiver, respectively.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is drawing showing the processing sequence of the encryption equipment concerning the gestalt of operation of the 1st of this invention.

[Drawing 2] It is the block diagram showing the hardware configuration of the 1st encryption IC 54 shown in drawing 1 .

[Drawing 3] It is drawing showing the processing sequence of the encryption equipment concerning the gestalt of operation of the 2nd of this invention.

[Drawing 4] It is drawing showing the processing sequence of the encryption equipment concerning the gestalt of operation of the 3rd of this invention.

[Drawing 5] It is drawing showing the processing sequence of the encryption equipment concerning the gestalt of operation of the 4th of this invention.

[Drawing 6] It is the block diagram showing the hardware configuration of the 1st encryption IC 94 shown in drawing 5 .

[Drawing 7] It is drawing showing the example of application to the concrete communication system of the encryption equipment concerning this invention.

[Drawing 8] It is the block diagram showing the configuration of the optical disk drive equipment 110 shown in drawing 7 .

[Drawing 9] It is drawing showing a general view of the circuit board mounted in the interior of this optical disk drive equipment 110.

[Drawing 10] It is the block diagram showing the configuration of the picture reproducer 111 shown in drawing 7 .

[Drawing 11] It is drawing showing the processing sequence of the one direction authentication concerning the 1st conventional technique.

[Drawing 12] It is drawing showing the processing sequence of the bidirectional authentication concerning the 2nd conventional technique.

[Description of Notations]

51, 71, 81, 91 The 1st device

52, 72, 82, 92 The 2nd device

53, 73, 83, 93 MPU of the 1st device

54, 74, 84, 94 1st encryption IC

55, 75, 85, 95 MPU of the 2nd device

56, 76, 86, 96 2nd encryption IC

59 Data Transfer Key K Generation Section

60,101 Random-number generation section

61,100 External I/F section

62,102 Random-number storing section

63 Bond Part

64,103 Authentication key S storing section

65, 66, 68,104,105,107 Switch

67,106 E function

69 Separation Section

70 Data Transfer Key K Storing Section

108 Comparator

110 Optical Disk Drive Equipment

111 Picture Reproducer

121 SCSI Controller

122 Control Section

123 Encryption IC

124 MPU

125 Optical Head

130 SCSI Controller

131 MPU

132 Encryption IC

133 MPEG Decoder

134 AV Signal-Processing Section

特開平10-51439

(43) 公開日 平成10年(1998) 2月20日

(51) Int. Cl. ⁴	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/10			H 0 4 L 9/00	6 2 1 A
G 0 9 C 1/00	6 6 0	7259-5 J	G 0 9 C 1/00	6 6 0 A
H 0 4 L 9/08			H 0 4 L 9/00	6 0 1 A
9/32				6 0 1 C
				6 0 1 E
審査請求 未請求 請求項の数22 O L (全 22 頁) 最終頁に続く				

(21) 出願番号 特願平9-129972

(22) 出願日 平成9年(1997) 5月20日

(31) 優先権主張番号 特願平8-126751

(32) 優先日 平8(1996) 5月22日

(33) 優先権主張国 日本 (J P)

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 松崎 なつめ

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 原田 俊治

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 館林 誠

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

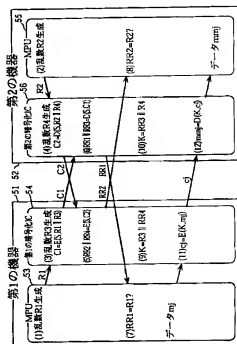
(74) 代理人 弁理士 中島 司朗

(54) 【発明の名称】 暗号化装置

(57) 【要約】

【課題】 規模の小さな暗号化 I C を備え、機器間通信の安全性を確保するための必要最小限の機能を有する暗号化装置を提供する。

【解決手段】 第1の機器 5 1 において、第1の暗号化 I C 5 4 は、第2の機器を認証する過程 (ステップ (1)、(3)、(6)、(7)) で生成した乱数 R 3 と、自らの正当性を第2の機器 5 2 に対して証明する過程 (ステップ (2)、(4)、(5)、(8)) で獲得した乱数 R 4 とを結合することで時変のデータ転送鍵を生成し (ステップ (9))、そのデータ転送鍵を用いてデジタル著作物を暗号化し、第2の機器 5 2 に転送する (ステップ (11))。



【特許請求の範囲】

【請求項1】 データ転送鍵の共有化とそのデータ転送鍵を用いた暗号通信を行なう機器に備えられる暗号化装置であって、

前記データ転送鍵の共有化のための第1乱数を生成する第1乱数生成手段と、

前記第1乱数生成手段により生成された第1乱数を保持する第1乱数保持手段と、

前記第1乱数生成手段により生成された第1乱数を前記暗号通信の相手機器に送信する第1送信手段と、

前記第1乱数保持手段に保持された第1乱数を用いて時変の前記データ転送鍵を生成するデータ転送鍵生成手段と、
暗号通信の対象となる転送データに対して前記データ転送鍵を用いて暗号化する転送データ暗号化手段とを備え、

前記第1乱数生成手段、前記第1乱数保持手段、前記データ転送鍵生成手段及び前記転送データ暗号化手段は、1個のIC内の回路で実現され、

前記第1乱数保持手段は、前記ICの外部からアクセスできない領域に前記第1乱数を保持することと特徴とする暗号化装置。

【請求項2】 前記暗号化装置はさらに、前記第1乱数生成手段により生成された第1乱数を暗号化する第1暗号化手段を備え、

前記第1暗号化手段は、前記IC内の回路で実現され、前記第1送信手段は、前記第1暗号化手段で暗号化された第1乱数を前記相手機器に送信することと特徴とする請求項1記載の暗号化装置。

【請求項3】 前記機器は、チャレンジレスポンス型の認証プロトコルに基づく通信により相互に前記相手機器が正当な機器であることを認証し合うものであり、前記暗号化装置はさらに、前記相手機器に送信するチャレンジデータ用の第2乱数を生成する第2乱数生成手段と、

前記チャレンジデータに対して前記相手機器から返信されてきたレスポンスデータと前記第2乱数とが一致するか否かを判断し、一致した場合に前記相手機器は正当な機器であると認証する認証手段とを備え、

前記データ転送鍵生成手段は、前記認証がなされた場合に前記データ転送鍵を生成することと特徴とする請求項2記載の暗号化装置。

【請求項4】 前記第2乱数生成手段及び前記認証手段は、前記IC外の回路で実現されていることを特徴とする請求項3記載の暗号化装置。

【請求項5】 前記暗号化装置はさらに、前記相手機器から送られてきた暗号化された結合データを復号化する復号化手段と、

復号化された結合データをレスポンスデータに相当する第1分離データと残る第2分離データとに分離する分離

手段と、

前記第1分離データを前記相手機器に返信する第2送信手段とを備え、

前記第1暗号化手段は、前記第1乱数と前記第2乱数とを結合し、その結果得られた結合データを暗号化し、前記データ転送鍵生成手段は、前記第1乱数と前記第2分離データとを結合することにより、前記データ転送鍵を生成し、

前記復号化手段及び前記分離手段は、前記IC内の回路で実現されていることを特徴とする請求項4記載の暗号化装置。

【請求項6】 前記暗号化装置はさらに、前記第2乱数をチャレンジデータとして前記相手機器に送信する第2送信手段と、

前記相手機器から送られてきた暗号化された結合データを復号化する復号化手段と、
復号化された結合データをレスポンスデータに相当する第1分離データと残る第2分離データとに分離する分離手段とを備え、

前記認証手段は、前記第1分離データを前記相手機器から返信されてきたレスポンスデータとして前記判断及び認証をし、

前記第1暗号化手段は、前記相手機器から送信されてきたチャレンジデータと前記第1乱数とを結合し、その結果得られた結合データを暗号化し、

前記データ転送鍵生成手段は、前記第1乱数と前記第2分離データとを結合することにより、前記データ転送鍵を生成し、

前記復号化手段及び前記分離手段は、前記IC内の回路で実現されていることを特徴とする請求項4記載の暗号化装置。

【請求項7】 前記転送データ暗号化手段による暗号化のアルゴリズムは、前記第1暗号化手段及び前記復号化手段の少なくとも1つのもとの同一であることを特徴とする請求項5又は6記載の暗号化装置。

【請求項8】 前記転送データ暗号化手段による暗号化のアルゴリズムは、前記第1暗号化手段及び前記復号化手段のいずれのものとも異なり、かつ、いずれのものよりも簡易であることを特徴とする請求項5又は6記載の暗号化装置。

【請求項9】 前記転送データ暗号化手段は、前記転送データを一定長のブロックに区切り、各ブロックに対して前記データ転送鍵の対応する部分を用いて暗号化することと特徴とする請求項8記載の暗号化装置。

【請求項10】 前記転送データ暗号化手段は、前記ブロックと前記データ転送鍵の対応する部分との排他的論理和をとることにより、前記暗号化を行なうことを特徴とする請求項9記載の暗号化装置。

【請求項11】 前記第1暗号化手段での暗号と前記復号化手段での復号とは、同一の変換アルゴリズムであ

ることを特徴とする請求項10記載の暗号化装置。

【請求項12】 前記第1暗号化手段及び前記復号化手段は、予め前記IC内に保持された鍵データを用いて前記暗号化及び復号化を行い、

その鍵データの一部は、前記IC内のマスクROM領域に格納され、残る一部は、前記IC内の追記ROM領域に格納されていることを特徴とする請求項11記載の暗号化装置。

【請求項13】 前記機器は、チャレンジレスポンス型の認証プロトコルに基づく通信により相互に前記相手機器が正当な機器であることを認証し合うものであり、前記暗号化装置はさらに、

前記チャレンジデータに対して前記相手機器から送られてきた暗号化された結合データを復号化する復号化手段と、

復号化された結合データをレスポンスデータに相当する第1分離データと残る第2分離データとに分離する分離手段と、

前記第1乱数と前記第1分離データとが一致するか否かを判断し、一致した場合に前記相手機器は正当な機器であると認証する認証手段と、

前記認証がなされた場合に前記第2分離データを暗号化する第2暗号化手段と、

暗号化された前記第2分離データをレスポンスデータとして前記相手機器に返信する第2送信手段とを備え、

前記データ転送鍵生成手段は、前記第1乱数と前記第2分離データとを結合することにより、前記データ転送鍵を生成し、

前記復号化手段、前記分離手段及び前記第2暗号化手段は、前記IC内の回路で実現されていることを特徴とする請求項2記載の暗号化装置。

【請求項14】 前記転送データ暗号化手段による暗号化のアルゴリズムは、前記第1暗号化手段、前記第2暗号化手段及び前記復号化手段の少なくとも1つのものと同一であることを特徴とする請求項13記載の暗号化装置。

【請求項15】 前記転送データ暗号化手段による暗号化のアルゴリズムは、前記第1暗号化手段、前記第2暗号化手段及び前記復号化手段のいずれのものとも異なり、かつ、いずれのものよりも簡易であることを特徴とする請求項13記載の暗号化装置。

【請求項16】 前記転送データ暗号化手段は、前記転送データを一定長のブロックに区切り、各ブロックに対して前記データ転送鍵の対応する部分を用いて暗号化することを特徴とする請求項15記載の暗号化装置。

【請求項17】 前記転送データ暗号化手段は、前記ブロックと前記データ転送鍵の対応する部分との排他的論理和をとることにより、前記暗号化を行なうことを特徴とする請求項16記載の暗号化装置。

【請求項18】 前記第1暗号化手段及び前記第2暗号

化手段での暗号化と前記復号化手段での復号化とは、いずれも同一の変換アルゴリズムであることを特徴とする請求項17記載の暗号化装置。

【請求項19】 前記第1暗号化手段、前記第2暗号化手段及び前記復号化手段は、予め前記IC内に保持された鍵データを用いて前記暗号化及び復号化を行い、その鍵データの一部は、前記IC内のマスクROM領域に格納され、残る一部は、前記IC内の追記ROM領域に格納されていることを特徴とする請求項18記載の暗号化装置。

【請求項20】 データ転送鍵の共有化とそのデータ転送鍵を用いた暗号通信を行なう送信機及び受信機から構成される通信システムであって、

それら送信機及び受信機は、チャレンジレスポンス型の認証プロトコルに基づく通信により相互に相手機器が正当な機器であることを認証し合うものであり、それぞれ、

チャレンジデータ用の第1乱数を生成する第1乱数生成手段と、

前記データ転送鍵用の第2乱数を生成する第2乱数生成手段と、

前記第1乱数と前記第2乱数を結合する結合手段と、前記結合データを暗号化する暗号化手段と、

暗号化された前記結合データを前記相手機器に送信する第1送信手段と、

前記相手機器の第1送信手段から送信された暗号化された結合データを受信する第1受信手段と、

受信した前記結合データを復号化する復号化手段と、復号化された前記結合データをレスポンスデータに相当する第1分離データと前記データ転送鍵用の第2分離データとに分離する分離手段と、

前記第1分離データをレスポンスデータとして前記相手機器に返信する第2送信手段と、

前記相手機器の第2送信手段から返信された第1分離データを受信する第2受信手段と、

受信した前記第1分離データと前記第1乱数とを比較し、一致している場合に前記相手機器を正当な機器と認証する比較手段と、

前記第2乱数と前記第2分離データとを結合することにより、前記データ転送鍵を生成するデータ転送鍵生成手段と、

前記認証がなされた場合に、生成された前記データ転送鍵を用いて前記相手機器と暗号通信を行なう暗号通信手段とを備えることを特徴とする暗号化装置。

【請求項21】 データ転送鍵の共有化とそのデータ転送鍵を用いた暗号通信を行なう送信機及び受信機から構成される通信システムであって、それら送信機及び受信機は、チャレンジレスポンス型の認証プロトコルに基づく通信により相互に相手機器が正当な機器であることを認証し合うものであり、それぞ

れ、
チャレンジデータ用の第 1 乱数を生成する第 1 乱数生成手段と、
前記第 1 乱数を前記相手機器に送信する第 1 送信手段と、
前記相手機器の第 1 送信手段から送信された第 1 乱数を受信する第 1 受信手段と、
前記データ転送鍵用の第 2 乱数を生成する第 2 乱数生成手段と、
受信した前記第 1 乱数と前記第 2 乱数を結合する結合手段と、
前記結合データを暗号化する暗号化手段と、
暗号化された前記結合データを前記相手機器に返信する第 2 送信手段と、
前記相手機器の第 2 送信手段から送信された暗号化結合データを受信する第 2 受信手段と、
受信した前記結合データを復号化する復号化手段と、
復号化された前記結合データをレスポンスデータに相当する第 1 分離データと前記データ転送鍵用の第 2 分離データに分離する分離手段と、
前記第 1 分離データと前記第 1 乱数生成手段で生成された前記第 1 乱数とを比較し、一致している場合に前記相手機器を正当な機器と認証する比較手段と、
前記第 2 乱数と前記第 2 分離データとを結合することで、前記データ転送鍵を生成するデータ転送鍵生成手段と、
前記認証がなされた場合に、生成された前記データ転送鍵を用いて前記相手機器と暗号通信を行なう暗号通信手段とを備えることを特徴とする暗号化装置。
【請求項 22】 データ転送鍵の共有化とそのデータ転送鍵を用いた暗号通信を行なう送信機及び受信機から構成される通信システムであって、
それら送信機及び受信機は、チャレンジレスポンス型の認証プロトコルに基づく通信により相互に相手機器が正当な機器であることを認証し合うものであり、
前記送信機は、
第 1 乱数を生成する第 1 乱数生成手段と、
前記第 1 乱数を暗号化する第 1 暗号化手段と、
暗号化された前記第 1 乱数を受信機に送信する第 1 送信手段とを備え、
前記受信機は、
暗号化された前記第 1 乱数を受信する第 1 受信手段と、
受信した前記第 1 乱数を復号化する第 1 復号化手段と、
第 2 乱数を生成する第 2 乱数生成手段と、
前記第 1 乱数と前記第 2 乱数を結合することで、結合データを生成する第 1 結合手段と、
前記結合データを暗号化する第 2 暗号化手段と、
暗号化された前記結合データを送信機に送信する第 2 送信手段とを備え、
前記送信機はさらに、

暗号化された前記結合データを受信する第 2 受信手段と、
受信した前記結合データを復号化する第 2 復号化手段と、
復号化された前記結合データを前記第 1 乱数に相当する第 1 分離データと前記第 2 乱数に相当する第 2 分離データとに分離する分離手段と、
前記第 1 乱数と前記第 1 分離データとを比較し、一致している場合に前記受信機を正当な機器と認証する第 1 比較手段と、
前記認証がなされた場合に前記第 2 分離データを暗号化する第 3 暗号化手段と、
暗号化された前記第 2 分離データを前記受信機に送信する第 3 送信手段と前記第 1 乱数生成手段で生成された第 1 乱数と前記分離手段で得られた第 2 分離データとを結合することで、前記データ転送鍵を生成する第 1 データ転送鍵生成手段とを備え、
前記受信機はさらに、
暗号化された前記第 2 分離データを受信する第 3 受信手段と、
受信した前記第 2 分離データを復号化する第 3 復号化手段と、
復号化された前記第 2 分離データと前記第 2 乱数とを比較し、一致している場合に前記送信機を正当な機器と認証する第 2 比較手段と、
前記認証がなされた場合に前記第 1 復号化手段で得られた前記第 1 乱数と前記第 2 乱数生成手段で生成された第 2 乱数とを結合することで、前記データ転送鍵を生成する第 2 データ転送鍵生成手段とを備え、
前記送信機はさらに、
前記第 1 データ転送鍵生成手段で生成されたデータ転送鍵を用いて転送データを暗号化する第 4 暗号化手段と、
暗号化された転送データを前記受信機に送信する第 4 送信手段とを備え、
前記受信機はさらに、
暗号化された前記転送データを前記送信機から受信する第 4 受信手段と、
前記第 2 データ転送鍵生成手段で生成されたデータ転送鍵を用いて転送データを復号化する第 4 復号化手段とを備えることを特徴とする暗号化装置。
【発明の詳細な説明】
【0001】
【発明の属する技術分野】本発明は、秘密鍵を共有して暗号通信を行なう通信機器に備えられる暗号化装置に関し、特に、小さい回路規模で実現することができる暗号化装置に関する。
【0002】
【従来の技術】通信路を介して通信されているデータが通信路上で不正にコピーされたり改変されることを防ぐことが必要となる場合が数多くある。例えば、映画など

の著作物がデジタル化されさらに情報圧縮され、さらに光ディスク上にデジタル記録されており、これが光ディスク再生装置により電気情報として取り出され、取り出されたデジタル情報が情報伸長装置により伸長され、映像音響再生装置により再生されるような場合である。

【0003】ここで光ディスク再生装置と情報伸長装置は別々の機器として分離しており、その間がデジタル通信路によりデータ通信される場合、この通信データが著作権者の許可なくデジタル情報記録装置により記録され、さらにデジタル情報複製装置により複製されるものであれば、その映画の著作物が不正に複製されることになり、著作権の侵害が起こる。従って通信路を介して通信されているデータが通信路上で不正にコピーされることを防がなければならない。機器内の回路や部品の仕様が一般には公開されないのに対し、データ通信のための電気的特性や信号形式は一般に公開される場合が多いので通信路におけるデータの不正コピーやそれに引き続くデータの改変が大きな問題になる。

【0004】このような不正行為を排除して安全な通信を確保するための技術については従来より様々なものが知られている。最も代表的なものには相手認証技術を用いるものである。これは基本的にはデータを送信する側が受信する側の正当性を認証し、正当な受信者であることが確認できたときのみにデータを送信することで、デジタル著作物が不正な機器に受信されることを防止するものである。

【0005】なお、この場合の受信者のように自らの正当性を証明する側を証明者と呼び、またこの場合の送信者のように相手の正当性を確認する側を認証者と呼ぶ。また、前述の光ディスク記録再生に関する機器のような場合では、特定の機器の間で認証が成功するか否かということよりも、それら機器が光ディスク関連機器の業界によって定められた規格に準拠したものであるか否かが問題となる。従ってこのような場合では、「正当性」とは「所定の規格に準拠すること」を意味する。

(第1の従来技術) 第1の具体的な従来技術として、国際標準規格ISO/IEC9798-2に記載される暗号技術を用いた一方認証方法がある。

【0006】この認証方法は証明者が認証鍵と呼ばれる秘密のデータを持つことを、その鍵自身を知らせることなく認証者に対して証明することを基本としている。そのためにまず認証者があるデータを選びこれを証明者に対して投げかける。この行為をチャレンジ、投げかけたデータをチャレンジデータと呼ぶ。これに対して証明者は、予め所有していた暗号変換と認証鍵を用いて前記チャレンジデータを暗号化する。そして、暗号化したデータを認証者に返す。この行為をレスポンス、そのデータをレスポンスデータと呼ぶ。

【0007】このレスポンスデータを受信した認証者

は、証明者が所有している暗号変換の逆変換である復号変換と認証鍵を共有しており、証明者から返信されてきたレスポンスデータをその認証鍵と復号変換を用いて復号化する。この結果が前記チャレンジデータと一致すれば受信者は正規の認証鍵を持つものと判断し、証明者の正当性を認証する。一方認証鍵とは一方の側がその正当性を他方に証明することを意味する。

【0008】ここで、暗号変換Tとは、鍵データSにより定まる平文集合から暗号文集合への写像である。平文をXとしたとき暗号文をT(S, X)と書く。同じ鍵データSにより定まる暗号文集合から平文集合への写像である逆変換TINVとの間には、 $TINV(S, T(S, X)) = X$ の関係がある。これは平文Xを暗号変換し、これを逆変換すると元に戻ることを意味している。暗号変換の逆変換を復号変換と呼ぶ。暗号変換であるためには鍵Sの知識がないときに暗号文T(S, X)から平文Xを求めるのが困難であることが必要である。なお、慣例により暗号変換をE(S,), 復号変換をD(S,)と記す。

【0009】図11は、前記規格に記載されている認証方法の一例を示す図である。図11では、第1の機器11から第2の機器12にデジタル著作物mjを転送する場合が示されている。ここでは、第1の機器11が第2の機器12の正当性を確認する。以下の従来の一方認証方法の動作を同図に示されたステップ番号に従って説明する。

【0010】(1) 第1の機器11は、乱数R1を生成する。そしてこれをチャレンジデータとして通信路を介して第2の機器12に送信する。

(2) 第2の機器12はこの乱数を受けると、第2の機器12に格納されている秘密の認証鍵Sを暗号鍵としてこの乱数を暗号化する。そしてその結果C1をレスポンスデータとして通信路を介して第1の機器11に送信する。

【0011】(3) 第1の機器11はこのレスポンスデータを受け取ると、第1の機器11に格納されている認証鍵Sを復号鍵としてこのレスポンスデータC1を復号化する。

(4) 第1の機器11は、復号の結果RR1を第1の機器11内に一時保管されている乱数R1と比較する。これが一致すれば第1の機器11は第2の機器12の機器が同じ認証鍵Sを保有するものと考え、通信相手が正当なものであると認証する。一方、一致しなければ通信相手が正当なものではないものと判断して処理を中断する。

【0012】(5) 第1の機器11は第2の機器12を正当なものとして認証した後、デジタル著作物を通信路を介して第2の機器12に送信する。もしも、第2の機器12の代わりに認証鍵Sを有さない第3の機器が通信路に接続されている場合には、その第3の機器は上記ステップ

(2)で正しい値のデータC1を作成することができず、結果としてステップ(3)で復号の結果RR1が前記R1と一致しないため、ステップ(4)において第1の機器11はデジタル著作物をその第3の機器に伝送しない。

【0013】なお、第1の機器11と第2の機器12の間でいつも同じチャレンジデータとレスポンスデータが用いられるならば、そのことを知った不正な第3の機器が第2の機器12になりますことが考えられる。これを避けるために第1の機器11からは毎回異なるチャレンジデータ(乱数)を送っている。

(第2の従来技術)とところで、上記第1の従来技術では、例えば認証の後、ハードディスク装置に記憶されている偽りのデータを正規の認証鍵を有する第2の機器12に対して不正に送出することも可能である。この問題を解決するため、第1の機器11が第2の機器12の正当性を確認すると同時に、第2の機器12も第1の機器11の正当性を確認することが必要となる。

【0014】また、双方の機器が認証した後にデジタル著作物を通信路を介して第2の機器12に伝送している最中に、この通信路上のデータを抜きとり、これを例えばハードディスク装置に記憶することが考えられる。もちろんこのためには通信路上の信号の電気的特性やデータ形式などの知識が必要であるが、それらの知識は一般に特に秘密にされている情報ではないので、そのデジタル著作物の抜きとりは技術的に十分に可能である。そのため、認証だけでは不十分であり、認証が成功した後に、各機器間でランダムに生成した新たな鍵を共有し、その鍵を用いてデジタル著作物を暗号化して転送する暗号通信をすることが必要になる。なお、デジタル著作物等の転送すべきデータを暗号化するための秘密鍵を、以下、「データ転送鍵」と呼ぶ。

【0015】以下、上記第1の従来技術である一方認証を拡張し、双方認証とデータ転送鍵の共有化と暗号通信とを行なう第2の従来技術を説明する。図12は、この双方認証を実現する装置の一例を示す。図12には、第1の機器21から第2の機器22にデジタル著作物m]を暗号化した後に転送する場合が示されている。

【0016】以下この従来の双方認証とデータ転送鍵の共有化の動作を同図に示されたステップ番号に従って説明する。

(1) 第1の機器21は乱数R1を生成する。これは第1のチャレンジデータとしての意味を持つ。そしてこれを通信路を介して第2の機器22に送信する。ここで乱数R2は第2の機器22から第1の機器21への第2のチャレンジデータとしての意味を持つ。つまり、暗号文C1は第1のチャレンジデータに対するレスポンスデータと第2のチャレンジデータの両方の意味を持つ。

【0017】(2) 第2の機器22は乱数R2を生成し、それと第1の機器21から受けとった乱数R1とを結合することで結合データR1||R2を作成する。ここで記

号||は双方のデータを桁方向に並べて結合することを示す。そして第2の機器22の認証鍵Sを暗号鍵として、この結合データR1||R2を暗号化し、その暗号文C1を第1の機器21に送信する。

【0018】(3) 第1の機器21は、第2の機器22から受信した暗号文C1を認証鍵Sを復号鍵として復号化し、その結果の上位を分離データRR1、下位を分離データRR2とする。

(4) 第1の機器21では、この分離データRR1を第1の機器21に一時記憶されている乱数R1と比較する。これが一致すれば通信相手が認証鍵Sを持っている正当な機器であると認証する。もしも一致しなければここで認証処理を中断する。

【0019】(5) 第1の機器21は、乱数Kを発生しこれをデータ転送鍵Kとして設定する。そして前記獲得した分離データRR2とこのデータ転送鍵Kを結合した結合データRR2||Kを第1の機器21の認証鍵Sで暗号化して、その暗号文C2を第2の機器22に送信する。

(6) 第2の機器22は、第1の機器21から受信した暗号文C2を認証鍵Sを用いて復号化し、その上位を分離データRRR2、下位を分離データKKとする。

【0020】(7) 第2の機器22では、この分離データRRR2を第2の機器22に一時記憶されている乱数R2と比較する。これが一致すれば通信相手が認証鍵Sを持っている正当な機器であると認証する。もしも一致しなければ、ここで認証処理を中断する。一方、復号化した分離データKKをデータ転送鍵Kとして設定する。

【0021】(8) 第1の機器21は、前記データ転送鍵Kを用いてデジタル著作物を暗号化し、通信路を介して第2の機器22に送信する。

(9) 第2の機器22ではこれを前記データ転送鍵KKを用いて復号化し、もとのデジタル著作物を獲得する。ここで、もしも第1の機器21が正規の認証鍵Sを有し、第2の機器22が正規の認証鍵を有している場合には、ステップ(4)で第1の機器21は通信相手が正規の認証鍵を有していないものと判断し、認証処理を中断できる。また第1の機器21が正規の認証鍵を有しておらず、第2の機器22は正規の認証鍵を有している場合には、ステップ(7)において第2の機器22は通信相手が正規の認証鍵を有していないものと判断し、認証処理を中断できる。このようにしてデジタル著作物が不正な機器に流出することを防止すると同時に不正な機器から正当な機器に流入することも防止することができる。

【0022】さらに、第1の機器21も第2の機器22も正当な認証鍵を有している場合において前記認証処理が完了したステップ(8)においてデジタル著作物が通信路上を伝送されている際に、もし、そのデジタル著作物が電氣的にコピーされ、デジタル蓄積装置に蓄積された場合であっても、そのデジタル著作物は暗号化されているので、無意味なデジタルデータとなっており、元の

デジタル著作物は有効に保護される。

【0023】以上のように、暗号技術を用いた双方向認証が首肯よく行われるには、第1の機器21及び第2の機器22の内部に格納されている認証鍵が不正を行おうとするものに容易に分からないことが必須の条件となる。また、チャレンジデータのための乱数の生成部やデータ転送鍵Kの生成部が外部からアクセス不可なこと、変更できないことが必要である。

【0024】それら構成要素の秘密性を確保する最も効果的な方法は、上記の認証やデータ転送鍵の共有化及び暗号通信を行う部分をICとして実現する方法である。ICを解析するには一般に多大な労力がかかるので、認証鍵などが容易には解読されないからである。

【0025】

【発明が解決しようとする課題】ところが、上記の第2従来技術における第1の機器21をICで実現するためには、そのようなIC（以下、「暗号化IC」という。）は次の部分を備えることが必要である。

- ・乱数R1を生成する乱数生成部
- ・暗号文C1を復号化するための復号部
- ・認証鍵Sを格納する部分
- ・乱数R1と分離データRR1を比較するための比較部
- ・データ転送鍵Kを生成するための乱数生成部
- ・分離データRR2とデータ転送鍵Kを結合して暗号化するための暗号部
- ・データ転送鍵Kを格納する部分
- ・データ転送鍵Kを用いてデジタル著作物を暗号化する暗号部

第2の機器22についてもこれと同程度の規模のハードウェアが必要である。

【0026】このように、上記従来の認証方式をICで実現したのでは、2つの乱数生成部、2つの変換部（復号部と暗号部）非常に多くの機能を持たなければならないために、回路規模が大きくなり結局機器のコストアップにつながるという問題点を有する。また、上記第2従来技術ではデータを暗号化するためのデータ転送鍵Kは第1の機器21が生成しているが、相互認証が必要とされると同じ理由により、この鍵は双方の機器が生成した値を反映するほうが望ましい。

【0027】以上説明したように、機器間の回線を保護するためには、認証等の機能やそのための秘密の情報をICに封じ込めて実現する方法が効果的である。しかし、従来の方法において、相互認証の部分、データ転送鍵の共有化の部分及びデータ暗号化の部分すべて1つのICで実現するのは、そのICの規模は非常に大きくなってしまい、コストアップにつながる。

【0028】そこで、本発明は、規模の小さな暗号化ICを備え、機器間通信の安全性を確保するための必要最小限の機能を有する暗号化装置を提供することを第1の目的とする。ここで暗号化ICは次の機能を有する。

(1) 認証鍵を安全に格納する。その鍵は外部からのアクセスにより書き換え及び読み出しがなされない。

【0029】(2) データ転送鍵を安全に共有する。その鍵は外部からのアクセスにより書き換え及び読み出しがなされない。

(3) 但し、通信システムの安全性に関連しない部分を暗号化ICに備えないことにより、暗号化ICの規模を最小とする。また、本発明の第2の目的は、規模の小さな暗号化ICを用いて実現するのに好適であり、かつ、安全性の高い暗号通信システムを提供することである。

【0030】

【課題を解決するための手段】上記第1の目的を達成するために本発明は、データ転送鍵の共有化とそのデータ転送鍵を用いた暗号通信を行なう機器に備えられる暗号化装置であって、前記データ転送鍵の共有化のための第1乱数を生成する第1乱数生成手段と、前記第1乱数生成手段により生成された第1乱数を保持する第1乱数保持手段と、前記第1乱数生成手段により生成された第1乱数を前記暗号通信の相手機器に送信する第1送信手段と、前記第1乱数保持手段に保持された第1乱数を用いて時変の前記データ転送鍵を生成するデータ転送鍵生成手段と、暗号通信の対象となる転送データに対して前記データ転送鍵を用いて暗号化する転送データ暗号化手段とを備え、前記第1乱数生成手段、前記第1乱数保持手段、前記データ転送鍵生成手段及び前記転送データ暗号化手段は、1個のIC内の回路で実現され、前記第1乱数保持手段は、前記ICの外部からアクセスできない領域に前記第1乱数を保持することを特徴とする。

【0031】これにより、データ転送鍵の生成に直接関連する第1乱数は外部からアクセスできない暗号化ICの内部に保持されるので、時変のデータ転送鍵は機器に安全に共有され、暗号通信が行われる。また、暗号化ICは、機器間通信の安全性を確保するための必要最小限の機能を持つので、小さな回路で実現することができる。

【0032】また、上記第2の目的を達成するために本発明は、データ転送鍵の共有化とそのデータ転送鍵を用いた暗号通信を行なう送信機及び受信機から構成される通信システムであって、それら送信機及び受信機は、チャレンジレスポンス型の認証プロトコルに基づく通信により相互に相手機器が正当な機器であることを認証し合うものであり、それぞれ、チャレンジデータ用の第1乱数を生成する第1乱数生成手段と、前記第1乱数と前記第2乱数を結合する結合手段と、前記結合データを暗号化する暗号化手段と、暗号化された前記結合データを前記相手機器に送信する第1送信手段と、前記相手機器の第1送信手段から送信された暗号化された結合データを受信する第1受信手段と、受信した前記結合データを復号化する復号化手段と、復号化された前記結合

データをレスポンスデータに相当する第1分離データと前記データ転送鍵用の第2分離データに分離する分離手段と、前記第1分離データをレスポンスデータとして前記相手機器に返信する第2送信手段と、前記相手機器の第2送信手段から返信された第1分離データを受信する第2受信手段と、受信した前記第1分離データと前記第1乱数とを比較し、一致している場合に前記相手機器を正当な機器と認証する比較手段と、前記第2乱数と前記第2分離データとを結合することで、前記データ転送鍵を生成するデータ転送鍵生成手段と、前記認証がなされた場合に、生成された前記データ転送鍵を用いて前記相手機器と暗号通信を行なう暗号通信手段とを備えることを特徴とする。

【0033】これにより、送信機及び受信機間で相互認証が行われと共にデータ転送鍵が生成されること、データ転送鍵の生成に直接関連する乱数はそのままでは送受信されないこと、及び、データ転送鍵の生成に直接関連する2つの乱数はそれぞれ送信機及び受信機から提供されたものであることから、規模の小さな暗号化ICを用いて実現するのに好適であり、かつ、安全性の高い暗号通信システムが実現される。

【0034】

【発明の実施の形態】

【実施の形態1】図1は、本発明に係る暗号化装置を備えた第1の機器と第2の機器間で相互認証とデータ転送鍵の共有化とデータの暗号通信とを行って実施の形態1における処理シーケンスを示す図である。

【0035】図1では、第1の機器51から第2の機器52にデジタル著作物mjを転送する場合が示されている。なお、図1には、各機器51、52が備える暗号化装置だけが示されており、暗号化装置と直接に関連しない他の構成要素（送受信部やデジタル著作物の処理系等）は省略されている。第1の機器51に備えられた本発明に係る暗号化装置は、大きく分けてMPU53と第1の暗号化IC54とから構成される。

【0036】MPU53は、この暗号化装置に固有の制御プログラムを保持するROMとその制御プログラムを実行する汎用マイクロプロセッサとRAM等からなり、データ転送鍵の共有化に直接的には関与しない処理（図中のステップ(1)、(7)）を行なう。第1の暗号化IC54は、1チップの半導体ICであり、データ転送鍵の共有化に直接的に關与する処理（図中のステップ(3)、(5)、(9)、(11)）を行なう。

【0037】同様に、第2の機器52に備えられた本発明に係る暗号化装置も、大きく分けてMPU55と第2の暗号化IC56とから構成される。MPU55は、この暗号化装置に固有の制御プログラムを保持するROMとその制御プログラムを実行する汎用マイクロプロセッサとRAM等からなり、データ転送鍵の共有化に直接的には関与しない処理（図中のステップ(2)、(8)）を行な

う。

【0038】第2の暗号化IC56は、1チップの半導体ICであり、データ転送鍵の共有化に直接的に關与する処理（図中のステップ(4)、(6)、(10)、(12)）を行なう。なお、この実施の形態においては、データ暗号化規格（DES:Data EncryptionStandard）に準拠した64ビットブロック暗号アルゴリズムEとその逆変換アルゴリズムDを用いている。以降では暗号アルゴリズムEを用いる変換を「暗号化」、逆変換アルゴリズムDを用いる変換を「復号化」と称する。

【0039】また、第1の暗号化IC54は暗号アルゴリズムEだけを、第2の暗号化IC56は逆変換アルゴリズムDだけを備える。これは、各暗号化IC54、56の規模を削減すること、安全性のためである。以下、図1に示されたステップ番号に従って、実施の形態1における暗号化装置の動作を説明する。

【0040】(1) 第1の機器51のMPU53において乱数R1（32ビット）を生成して、記憶するとともに第1の暗号化IC54に渡す。

(2) ステップ(1)と同様に、第2の機器52のMPU55において乱数R2（32ビット）を生成して、記憶するとともに第2の暗号化IC56に送信する。

【0041】(3) 第1の暗号化IC54において、乱数R3（32ビット）を生成、外部よりアクセスできない領域に格納する。そして、前記MPUで生成した乱数R1と前記乱数R3を結合してE関数で暗号化する。ここで、記号“||”は2つの乱数を桁方向に結合して64ビット（乱数R1を上位32ビット、乱数R3を下位32ビット）とすることを示している。また、暗号化には第1の暗号化IC54及び第2の暗号化IC56で予め共通に保持している秘密の認証鍵Sを用いる。第1の暗号化IC54は、第1の機器51の送信部（図では示していない）を介して上記暗号結果C1を第2の機器52に送信する。

【0042】(4) ステップ(3)と同様に、第2の暗号化IC56において、乱数R4（32ビット）を生成して、外部よりアクセスできない領域に格納する。前記MPUで生成した乱数R2と前記乱数R4を結合して逆変換アルゴリズムDで復号化する。復号には前記認証鍵Sを用いる。第2の暗号化IC56は、第2の機器52の送信部（図では示していない）を介して復号結果C2（64ビット）を第1の機器51に送信する。

【0043】(5) 第1の暗号化IC54において、前記第2の機器52から受信した復号文C2を前記E関数を用いて前記認証鍵Sで暗号化する。そして、得られた64ビットをその上位32ビットである分離データRR2と下位32ビットである分離データRR4に分離する。さらに、分離データRR2は第1の機器51の送信部を介して第2の機器52に送信し、一方、分離データRR4は外に出さずに第1の暗号化IC54内の外部からア

クセスできない領域に格納する。

【0044】なお、第1の暗号化IC54及び第2の暗号化IC56が互いに正規なものであり同じ認証鍵Sを保持している場合には、前記分離データRR2は前記第2の機器52のMPU55が生成した乱数R2と一致し、前記分離データRR4は前記第2の暗号化IC56が内部に格納している乱数R4と一致する。

(6) ステップ(5)と同様に、第2の暗号化IC56において、前記第1の暗号化IC54から受信した暗号文C1を前記逆変換アルゴリズムDを用いて前記認証鍵Sで復号化する。そして、得られた64ビットをその上位32ビットである分離データRR1と下位32ビットである分離データRR3に分離する。さらに、分離データRR1は第2の機器52の送信部を介して第1の機器51に送信し、一方、分離データRR3は外に出さずに第2の暗号化IC56内の外部からアクセスできない領域に格納する。

【0045】なお、第1の暗号化IC54及び第2の暗号化IC56が互いに正規なものであり同じ認証鍵Sを保持している場合には、前記分離データRR1は前記乱数R1と一致し、前記分離データRR3は前記乱数R3と一致する。

(7) 第1の機器51のMPU53において前記ステップ(1)で記憶していた乱数R1と前記第2の機器52から受信した分離データRR1とを比較し、一致している場合には、第2の暗号化IC56及びそれを備えた第2の機器52を正当な機器と認証する。

【0046】(8) ステップ(7)と同様に、第2の機器52のMPU55において前記ステップ(2)で記憶していた乱数R2と前記第2の機器52から受信した分離データRR2とを比較し、一致している場合には、第1の暗号化IC54及びそれを備えた第1の機器51を正当な機器と認証する。

(9) 第1の暗号化IC54において、前記ステップ(3)で記憶しておいた乱数R3と前記分離データRR4を結合することでデータ転送鍵Kを作成する。ここでは、乱数R3を上位の32ビット、分離データRR4を下位の32ビットとするデータ転送鍵K(64ビット)を生成する。なお、このデータ転送鍵Kは、2つの乱数の結合であるので、時変、即ち、新たにランダムに生成された鍵と言える。

【0047】(10) ステップ(9)と同様に、第2の暗号化IC56において、前記分離データRR3と前記ステップ(4)で記憶しておいた乱数R4を結合することでデータ転送鍵Kを生成する。ここでは、上記分離データRR3を上位の32ビット、上記ステップ(4)で記憶しておいた乱数R4を下位の32ビットとするデータ転送鍵K(64ビット)を生成する。このデータ転送鍵も時変の鍵である。

【0048】なお、ステップ(7)及びステップ(8)での相

互の認証が成功した場合には、ステップ(3)で生成された乱数R3とステップ(6)で得られた分離データRR3とは一致し、ステップ(4)で生成された乱数R4とステップ(5)で得られた分離データRR4とは一致することになるので、結果的に、ステップ(9)及びステップ(10)それぞれで生成されるデータ転送鍵Kは一致することになる。

【0049】(11) 第1の機器51の第1の暗号化IC54において、MPU53から送られてくるブロック化されたデジタル著作物m j (64ビット)を上記ステップ(9)で得られたデータ転送鍵Kを用いて暗号化し、得られた暗号文C j を第2の機器52に送信する処理を、転送すべき全てのデジタル著作物を送信し終えるまで繰り返す。

【0050】(12) ステップ(11)に対応して、第2の機器52の第2の暗号化IC56において、第1の機器51が送信した暗号化された上記デジタル著作物C j (64ビット)を受信し、上記ステップ(10)で得られたデータ転送鍵Kを用いて復号化し、得られたデジタル著作物mm j をMPU55に送る。この復号化は上記デジタル著作物C j が第1の機器51から送信されてくる限り繰り返す。

【0051】このようにして、実施の形態1の暗号化装置により、第1の機器51と第2の機器52間で相互認証とデータ転送鍵Kの共有化とデータの暗号通信とが行われる。以上の説明から明らかなように、上記実施の形態1の暗号化装置は、以下の特徴を有する。

【0052】第1の特徴は、データ転送鍵Kは暗号化ICの内部に安全に保護されていることである。具体的には、第1の機器51が備える暗号化装置であれば、データ転送鍵Kを生成するために直接的に用いられる2つのデータ、即ち、乱数R3と分離データRR4は以下の条件を満たす。

- ・乱数R3は、第1の暗号化IC54の内部で生成され、外部に出力されておらず、かつ、外部から読めない領域に保持されている。

- ・分離データRR4は、第1の暗号化IC54の内部で生成(分離生成)され、外部に出力されておらず、かつ、外部から読めない領域に保持されている。これらのことにより、データ転送鍵Kは暗号化IC内に保護されるので、暗号アルゴリズムE及び逆変換アルゴリズムDとして公開されているものを採用したとしても、第1の機器51及び第2の機器52間における暗号通信の安全性は保証される。

- 【0054】第2の特徴は、暗号化IC内に納められる回路は、必要最低限のものに留められていることである。具体的には、第1の機器51が備える暗号化装置であれば、以下の処理は、第1の暗号化IC54の外の回路、即ち、MPU53によって実現される。

- ・乱数R1の生成

・乱数R1と分離データRR1との比較
つまり、第1の暗号化IC54の回路規模が不必要に大きくなりないように配慮されている。これら2つの処理は、相手機器の認証に関するものであり、データ転送鍵Kの生成に直接的には関与していない。従って、たとえ、これら処理がIC外で実現されていることを利用して不正をしようとしても、第1の機器51に利益をもたらすような不正をはたらくことは不可能である。なお、第2の機器52からのチャレンジデータC2に対するレスポンスデータRR2の作成は暗号化IC内で行っている。

【0055】図2は、第1の暗号化IC54のハードウェア構成を示すブロック図である。第2の暗号化IC56も同程度のハードウェア規模で実現できる。外部I/F部61は、この第1の暗号化IC54の内部回路に外部からアクセスするための唯一の入出力ポートである。乱数生成部60は、32ビットの乱数R3を生成する。

【0056】乱数格納部62は、乱数生成部60で生成された乱数R3を保持する記憶回路である。結合部63は、乱数格納部62に格納された乱数R3を下位32ビットとし、外部I/F部61を介して入力された32ビットのデータR1を上位32ビットとして結合する。

【0057】認証鍵S格納部64は、予め与えられた認証鍵Sを保持する記憶回路である。スイッチ65、66は、それぞれ64ビット幅の3入力1出力マルチプレクサ、64ビット幅の2入力1出力マルチプレクサである。E関数67は、暗号アルゴリズムEに基づく暗号化回路である。スイッチ68は、64ビット幅の1入力3出力マルチプレクサである。

【0058】分離部69は、スイッチ68から出力された64ビットデータを上位32ビットRR2と下位32ビットRR4に分離する。データ転送鍵K生成部59は、乱数格納部62に格納された乱数R3を上位32ビットとし、分離部69で分離された分離データRR4を下位32ビットとして結合することで、データ転送鍵Kを生成する。

【0059】データ転送鍵K格納部70は、データ転送鍵K生成部59で生成されたデータ転送鍵Kを保持する記憶回路である。次に、この図2に示された各構成要素が図1に示された各ステップにおいてどのように動作するかを示す。図1のステップ(3)においては、乱数生成部60は乱数R3を生成して乱数格納部62に格納し、結合部63はその乱数R3と外部I/F部61を介して入力される乱数R1とを結合し、スイッチ65を介してE関数67に送る。E関数67は、認証鍵S格納部64からスイッチ66を介して認証鍵Sを受け取り、それを用いて結合部63から出力された結合データR1||R3を暗号化し、その結果C1をスイッチ68及び外部I/F部61を介して第2の機器52に出力する。

【0060】図1のステップ(5)及び(9)においては、外

部I/F部61を介して入力される復号文C2はスイッチ65を経てE関数に入力される。E関数67は、認証鍵S格納部64から認証鍵Sを受け取り、それを用いて復号文C2を暗号化し、スイッチ68を介して分離部69に送る。分離部69は、それを分離データRR2と分離データRR4に分離し、分離データRR2は外部I/F部61を介して外部に出力し、分離データRR4はデータ転送鍵K生成部59に送る。データ転送鍵K生成部59は、乱数格納部62に格納されていた乱数R3と分離部69から送られてきた分離データRR4とを結合することでデータ転送鍵Kを生成した後に、データ転送鍵K格納部70に格納する。

【0061】図1のステップ(11)においては、E関数67は、外部I/F部61及びスイッチ65を介して入力されるデジタル著作権物mjをデータ転送鍵K格納部70に格納されたデータ転送鍵Kを用いて暗号化し、その結果Cjをスイッチ68及び外部I/F部61を介して第2の機器52に出力する。なお、実施の形態1では、乱数や暗号文等の具体的なビット長やデータ構成を示したが、本発明はそれらに限定されるものではない。例えば、上記ステップ(5)において32ビットの乱数R1とR2を結合して64ビットとし、これを64ビット暗号関数Eに入力して64ビットの暗号文C1を求めると、この部分は、例えば、各乱数を64ビットとし、暗号関数Eによる暗号化を2回繰り返すことで128ビットの暗号文C1を生成する方式としてもよい。ただしこの場合には暗号文C1から乱数R1に関する部分とR2に関する部分が容易に切り離せないことが必要である。その方法の一つとしてはCBCモードのように連鎖に伴う暗号の方法がある。CBCモードについては、池野哲一、小山謙二共著「現代暗号理論」電子通信学会1986年のp70に詳しい。

【0062】また、実施の形態1では第1の暗号化IC54は暗号関数Eだけを、第2の暗号化IC56はその逆関数Dだけを備えることにより、ハードウェア規模を削減しているが、そのこと自体は、上述のように本発明の本質ではない。つまり、それら暗号化IC54、56に許容される回路規模や暗号化アルゴリズムの種類等との関連において決定すればよい事項であり、例えば、それぞれが暗号アルゴリズムEと逆変換アルゴリズムDの両方を所有し、乱数の暗号化に暗号アルゴリズムEを、相手機器から送付された情報の復号に逆変換アルゴリズムDを用いてもよい。本発明は、少なくともデータ転送鍵Kの生成に直接関わる構成要素をIC化することで秘密通信の安全性を確保している点に特徴があるからである。

【0063】また、実施の形態1において、例えば、ステップ(1)での乱数R1の生成を第1の暗号化IC54内で行ってもよい。このことにより、第1の暗号化IC54を暗号解読器として用いる可能性をなくし、より安

全な暗号化装置とすることができ。つまり、実施の形態1では、乱数R1は第1の暗号化IC54の外部で生成され、この乱数R1に基づいて第1の暗号化IC54は暗号文C1を出力する。この暗号文C1は、第1の暗号化IC54の内部で生成された乱数R3の影響を受けているが、もし乱数R3が十分にランダムな値でない場合には、第1の暗号化IC54を暗号解読器として悪用することが可能になってしまう。従って、乱数R1の生成を第1の暗号化IC54内で行うことで、以上述べた攻撃の可能性がなくなり、この暗号化装置はより安全なものになる。

(実施の形態2) 次に、図1に示された実施の形態1でのステップの変形例として、実施の形態2を示す。その目的や効果は実施の形態1と同じである。またハードウェア規模としても図2に示された実施の形態1と同程度である。実施の形態1ではチャレンジデータを暗号化しないでレスポンスデータを暗号化して送信したが、実施の形態2ではチャレンジデータを暗号化しレスポンスデータを暗号化しないで通信する。実施の形態1と相違する点を中心に説明する。

【0064】図3は、本発明に係る暗号化装置を備えた第1の機器71と第2の機器72間で相互認証とデータ転送鍵の共有化とデータの暗号通信とを行う実施の形態2における処理シーケンスを示す図である。図3では、第1の機器71から第2の機器72にデジタル著作物mを転送する場合が示されている。

【0065】MPU73、第1の暗号化IC74、MPU75及び第2の暗号化IC76は、実施の形態1におけるMPU53、第1の暗号化IC54、MPU55及び第2の暗号化IC56に対応し、処理手順の相違を除いて、ハードウェア構成等については実施の形態1の場合と同様である。以下、図3に示されたステップ番号に従って、実施の形態2における暗号化装置の動作を説明する。

【0066】(1) 第1の機器71のMPU73において乱数R1(32ビット)を生成して、記憶するとともに第1の機器71の送信部(図では示していない)を介して、第2の機器72に送信する。第2の機器72ではこれを第2の暗号化IC76に渡す。

(2) ステップ(1)と同様に、第2の機器72のMPU75において乱数R2(32ビット)を生成して、記憶するとともに第2の機器72の送信部(図では示していない)を介して、第1の機器71に送信する。第1の機器71ではこれを第1の暗号化IC74に渡す。

【0067】(3) 第1の暗号化IC74において、乱数R3(32ビット)を生成して、外部よりアクセスできない領域に格納する。前記第2の機器72から受信した乱数R2と前記乱数R3とを結合してE関数で暗号化する。暗号化には第1の暗号化IC74及び第2の暗号化IC76で予め共通に保持している秘密の認証鍵Sを用

いる。第1の暗号化IC74は、暗号化結果C1(64ビット)を第2の機器72に送信する。

【0068】(4) ステップ(3)と同様に、第2の暗号化IC76において、乱数R4(32ビット)を生成して、外部よりアクセスできない領域に格納する。前記第1の機器71から受信した乱数R1と前記乱数R4を結合して逆変換アルゴリズムDで復号化する。復号には前記認証鍵Sを用いる。第2の暗号化IC76は、復号結果C2(64ビット)を第1の機器71に送信する。

【0069】(5) 第1の暗号化IC74において、前記第2の暗号化IC76から受信した復号文C2を前記E関数を用いて前記認証鍵Sで暗号化する。その結果の64ビットデータのうち上位32ビットを分離データRR1、下位32ビットを分離データRR4とする。そして分離データRR1は第1の機器71のMPU73に渡し、一方分離データRR4は外に出さずに第1の暗号化IC74内の外部からアクセスできない領域に格納する。

【0070】なお、第1、第2の暗号化IC76が互いに正規なものであり同じ認証鍵Sを保持している場合には、前記分離データRR1は前記第1の機器71のMPU73が生成した乱数R1と同じになり、前記分離データRR4は第2の暗号化IC76が生成した乱数R4と同じになる。

(6) ステップ(6)と同様に、第2の暗号化IC76において、前記第1の暗号化IC74から受信した暗号文C1を前記逆変換アルゴリズムDを用いて前記認証鍵Sで復号化する。その結果の64ビットデータの上位32ビットを分離データRR2、下位32ビットを分離データRR3とする。そして分離データRR2は第2の機器72のMPU75に渡し、一方分離データRR3は外に出さずに第2の暗号化IC76内の外部からアクセスできない領域に格納する。

【0071】なお、第1、第2の暗号化IC76が互いに正規なものであり同じ認証鍵Sを保持している場合には、前記分離データRR2は前記第2の機器72のMPU75が生成した乱数R2と同じになり、前記分離データRR3は第1の暗号化IC74が生成した乱数R3と同じになる。

(7) 第1の機器71のMPU73において前記記憶していたR1と前記第1の暗号化IC74から受け取った分離データRR1を比較して一致している場合には、第2の暗号化IC76及び第2の暗号化IC76が含まれた第2の機器72を正当な機器と認証する。

【0072】(8) ステップ(8)と同様に、第2の機器72のMPU75において前記記憶していたR2と前記第2の暗号化IC76から受け取った分離データRR2を比較して一致している場合には、第1の暗号化IC74及び第1の暗号化IC74が含まれた第1の機器71を正当な機器と認証する。

(9) 第1の暗号化IC74内で前記乱数R3と前記分離データRR4を用いてデータ転送鍵Kを作成する。図では双方の結合をデータ転送鍵K(64ビット)としている。

【0073】(10) ステップ(10)と同様に、第2の暗号化IC76内で前記分離データRR3と前記乱数R4を用いて第1の暗号化IC74と同様にデータ転送鍵Kを作成する。図では双方の結合をデータ転送鍵K(64ビット)としている。

(11) 第1の機器71の第1の暗号化IC74において、MPU73から送られてくるブロック化されたデジタル著作物mj(64ビット)を上記ステップ(9)で得られたデータ転送鍵Kを用いて暗号化し、得られた暗号文Cjを第2の機器72に送信する処理を、転送すべき全てのデジタル著作物を送信し終わるまで繰り返す。

【0074】(12) ステップ(11)に対応して、第2の機器72の第2の暗号化IC76において、第1の機器71が送信した暗号化された上記デジタル著作物Cj(64ビット)を受信し、上記ステップ(10)で得られたデータ転送鍵Kを用いて復号化し、得られたデジタル著作物mmjをMPU75に送る。この復号化は上記デジタル著作物Cjが第1の機器71から送信されてくる限り繰り返す。

【0075】このようにして、実施の形態2の暗号化装置により、実施の形態1の場合と同様に、第1の機器71と第2の機器72間で相互認証とデータ転送鍵Kの共有化とデータの暗号通信が行われる。なお、上述したように、本実施の形態の暗号化装置と実施の形態1のものとはハードウェア構成において一致し、処理手順、即ち、各ハードウェア構成要素の接続と実行順序が異なるだけである。従って、本実施形態の暗号化装置の特徴やその変形例については、実施の形態1の場合と同様のことが言える。

(実施の形態3) 以上の実施の形態1及び2の暗号化装置には以下の共通点がある。

- (1) 双方の機器においてそれぞれ2つの乱数が生成され、その一方は認証用のみ使用され、他の一方はデータ転送鍵Kの生成用のみ使用される。
- (2) データ転送鍵Kの生成に使用される乱数はそのままの形で暗号化ICの外部に出力されることはなく、一方、認証用に使われる乱数は暗号化ICの外部に出力されて公開される。

【0076】これに対して、次に説明する実施の形態3の暗号化装置は、乱数をつだけ生成し、それを認証用とデータ転送鍵の生成用の両方の目的に使用する。これは、実施の形態1及び2に比べて、暗号化IC内の乱数生成の負担を軽減するためである。また、暗号化ICの内部において認証のための乱数生成と比較処理を行う。即ち、実施の形態1及び2と相違し、データ転送鍵の生成のみならず認証処理も含めて暗号化ICの内部回

路で行う。これは、上述したように、暗号化ICを暗号解読のために用いるという悪用に対処するためであり、暗号通信の安全性を高めることができる。

【0077】図4は、本発明に係る暗号化装置を備えた第1の機器71と第2の機器72間で相互認証とデータ転送鍵の共有化とデータの暗号通信を行う実施の形態3における処理シーケンスを示す図である。図4では、第1の機器81から第2の機器82にデジタル著作物mjを転送する場合が示されている。

【0078】なお、本実施の形態においても、実施の形態1及び2と同様に、各機器81、82に備えられた本発明に係る暗号化装置は、大きく分けてMPU83、85と暗号化IC84、86とから構成される。しかし、MPU83、85はデジタル著作物mjを暗号化IC84、86に渡すだけの機能を果たすので、実質的には、本発明に係る暗号化装置は暗号化IC84、86のみから構成されると言える。

【0079】第1の暗号化IC84及び第2の暗号化IC86は、実の形態1及び2と同様、1チップの半導体ICである。以下、図4に示されたステップ番号に従って、実施の形態3における暗号化装置の動作を説明する。

(1) 第1の暗号化IC84において乱数R1を生成して記憶するとともに、これをE間数で暗号化して第1の機器81の送信部(図では示していない)を介して、暗号文C1を第2の機器82に送信する。暗号化には第2の暗号化IC86と予め共通に保持している秘密の認証鍵Sを用いる。第2の機器82では受信した暗号文C1を第2の暗号化IC86に渡す。

【0080】(2) 第2の暗号化IC86では受信した暗号文C1を逆変換アルゴリズムDで復号化し復号文RR1を得る。第1の暗号化IC84及び第2の暗号化IC86が正規のものである場合にはこの復号文RR1は前記乱数R1と一致する。

(3) 第2の暗号化IC86において乱数R2を生成して記憶すると共に、これを前記復号文RR1と結合して前記逆変換アルゴリズムDで復号化する。復号には前記認証鍵Sを用いる。第2の暗号化IC86は復号文C2を第2の機器82の送信部(図では示していない)を介して、第1の機器81に送信する。第1の機器81ではこれを第1の暗号化IC84に渡す。

【0081】(4) 第1の暗号化IC84においては、前記復号文C2を前記E間数で暗号化し、その結果を分離データRRR1と分離データRR2に分離する。なお分離データRRR1は正当な機器でのやり取りの場合であれば、前記復号文RR1及び乱数R1と一致する。また分離データRR2は前記乱数R2と一致する。

(5) 第1の暗号化IC84内において、前記ステップ(1)で記憶していた乱数R1と前記分離データRRR1とを比較し、一致する場合には第2の暗号化IC86及

び第2の暗号化IC86を含んだ第2の機器82の正当性を認証する。

【0082】(6) 第1の暗号化IC84において、前記分離データRR2を前記E関数で暗号化し、第2の機器82に送信する。第2の機器82はこの暗号文C3を第2の暗号化IC86に送す。

(7) 第2の暗号化IC86において、前記暗号文C3を前記逆変換アルゴリズムDで復号化し、復号文RRR2を得る。

【0083】(8) 第2の暗号化IC86において、前記ステップ(3)で記憶している乱数R2と前記復号文RRR2を比較し、一致している場合には第1の暗号化IC84及び第1の暗号化IC84を含んだ第1の機器81の正当性を認証する。

(9) 第1の暗号化IC84において、前記乱数R1と前記分離データRR2を結合することでデータ転送鍵Kを生成する。

【0084】(10) 第2の暗号化IC86において、前記復号文RRR1と前記乱数R2を用いてデータ転送鍵Kを生成する。

(11) 第1の機器81の第1の暗号化IC84において、MPU83から送られてくるブロック化されたデジタル著作物mj(64ビット)を上記ステップ(9)で得られたデータ転送鍵Kを用いて暗号化し、得られた暗号文Cjを第2の機器82に送信する処理を、転送すべき全てのデジタル著作物を送信し終わるまで繰り返す。

【0085】(12) ステップ(11)に対応して、第2の機器82の第2の暗号化IC86において、第1の機器81が送信した暗号化された上記デジタル著作物Cj(64ビット)を受信し、上記ステップ(10)で得られたデータ転送鍵Kを用いて復号化し、得られたデジタル著作物mmjをMPU85に送る。この復号化は上記デジタル著作物Cjが第1の機器81から送信されてくる限り繰り返す。

【0086】このようにして、実施の形態3の暗号化装置により、実施の形態1及び2の場合と同様に、第1の機器71と第2の機器72間で相互認証とデータ転送鍵Kの共有化とデータの暗号通信とが行われる。なお、上記ステップ(1)(2)(6)(7)においては1つの乱数の暗号化、ステップ(3)(4)においては2つの乱数の結合の暗号化を行っている。64ビット幅のE関数と逆変換アルゴリズムDを用いる場合には、各乱数を32ビットとして、前者については残りの32ビットの入力に固定の32ビットの値をパディングするとよい。例えば、乱数を下位32ビットとし、上位32ビットを固定的に全てゼロとする等である。また後者については結合した64ビットをそのまま各関数に入力するとよい。

【0087】また、各乱数のビット長を倍の64ビットにする場合には、前者はそのまま関数に入力し、後者については各関数を2回繰り返して用い、例えばCBCモ

ードのように連鎖のある暗号を行えばよい。以上述べた実施の形態3においては、実施の形態1及び2とは異なり、認証のための乱数とデータ転送鍵の共有化のための乱数は兼用されている。そして、認証のための乱数生成や認証のための比較処理は暗号化IC内で行われている。従って、乱数はそのままは暗号化ICの外に現れないため、暗号化ICを解読器として用いる攻撃に対して、より安全である。また、このことにより、各乱数のビット数が少なくても十分な安全性を確保することができる。

(実施の形態4) 次に、実施の形態4に係る暗号化装置について説明する。

【0088】本装置は、暗号化ICのコンパクト化を追求した実施形態であり、一方認証を採用している点、及び、データ転送鍵が公開される点において、上記実施の形態1〜3と相違する。但し、暗号アルゴリズムE及びその逆変換アルゴリズムDは秘密にされていることを前提とする。図5は、第1の機器91から第2の機器92にデジタル著作物mjを送送する場合の処理シーケンスを示す図である。

【0089】図6は、第1の暗号化IC94のハードウェア構成を示すブロック図である。

(1) まず、第1の暗号化IC94の乱数生成部101はチャレンジデータとデータ転送鍵を兼用する乱数R1を生成し、乱数格納部102に格納すると共に、外部1/F部100を介して第2の機器92に送信する。

(2) 第2の暗号化IC96は、受信した乱数R1に対して、予め第1の暗号化IC94と共通に所有している認証鍵Sを用いて復号化し、得られた復号文C1を第1の機器91に送信する。

【0090】(3) 第1の暗号化IC94では、E関数106は、外部1/F部100及びスイッチ105を介して受信した復号文C1に対して、認証鍵S格納部103に予め格納された上記認証鍵Sと同じものを用いて暗号化する。その結果得られたデータRRR1は、スイッチ107を経て比較部108に送られ、ここで、乱数格納部102に保持されていた乱数R1と比較される。

【0091】(4) その結果一致している場合には、第2の機器92は正当な機器であると認証できるので、比較部108は、乱数格納部102に保持されていた乱数R1がデータ転送鍵として用いられるように、スイッチ104を制御する。

(5) E関数106は、MPU93から外部1/F部100及びスイッチ105を経て送られてくるデジタル著作物mjに対して、スイッチ104を経て送られてくる乱数R1を用いて暗号化し、スイッチ107及び外部1/F部100を介して第2の機器92に送信する。

【0092】(6) 第2の機器92の第2の暗号化IC96においては、第1の機器91から送られてきたデジタル著作物Cjに対して、上記ステップ(2)で受信した乱

数R1をデータ転送鍵として用いて復号化し、得られたデジタル著作物mmjをMPU95に送る。このようにして、本実施の形態では、実施の形態1～3の場合より少ないステップと構成要素により、認証とデータ転送鍵の共有化と暗号通信が実現される。

【0093】なお、本実施の形態では、第1の機器91から第2の機器92に送信された乱数R1がそのままデータ転送鍵として用いられているために、データ転送鍵は容易に第3者に知られる。ところが、そのデータ転送鍵を知った第3者がデジタル著作物Cjを盗聴し復号化しようとしても、上述したように暗号アルゴリズムE及びその逆変換アルゴリズムDは秘密にされているので、その試みは成功しない。

【0094】また、その第3者が都合のよい乱数R1を偽造することで暗号アルゴリズムを解読しようとしても、新たな乱数R1を乱数格納部102に格納できるのは乱数生成部101だけであり、この第1の暗号化IC94の外部から新たな乱数R1を乱数生成部101に格納する手段は存在しないので、その試みも成功しない。このように、暗号アルゴリズム及びその逆変換アルゴリズムが秘密にされるならば、本実施の形態のようなコンパクトな暗号化ICによっても認証とデータ転送鍵の生成と暗号通信を実現することができ。

【0095】なお、上記実施の形態1～4において、認証鍵Sを暗号化ICに設定する（記憶させる）方法としては以下が好ましい。つまり、認証鍵Sの一部は暗号化ICの製造時に予め設定しておき、残る部分はその暗号化ICの製造後に書き込む方法である。具体的には、認証鍵S格納部64の一部は、認証鍵Sの一部を予め書き込んだマスクROMで構成し、残る部分は、プログラマブルに書き込み可能な追記ROMで構成する。

【0096】これは、マスクROMのみで構成した場合には、最終的な暗号化ICの作成のために人手を介さないために安全である反面、リパースエンジニアリングによるチップ解析で設定値の解析が容易であるという欠点があり、一方、追記ROMのみで構成した場合には、設定値のリパースエンジニアリングによる解析が困難である反面、設定に人手を介するためミスが混入したり不正が可能となるという欠点があるので、それら両方の欠点を補うためである。

【0097】また、上記実施の形態1～4の暗号通信における暗号アルゴリズムの具体例として、次のようなものであってもよい。送信側でデジタル著作物を64ビットのブロックに分割し、前記データ転送鍵K（64ビット）とビットごとの排他的論理和をとる。その結果を暗号文とする。受信側でも同様に、受信した64ビットの暗号文とデータ転送鍵Kとの排他的論理和をとればよい。これによって、もとのブロックに復号される。

【0098】また、データ転送鍵Kを固定とするのではなく、それらブロックごとに、用いられるデータ転送鍵

Kを送信側と受信側で同期をとりながら更新していく方法もある。その更新のために、前記E関数や逆変換アルゴリズムDを用いてもよい。ブロック内の暗号/復号は先に述べた排他的論理和であってよい。また、上記実施の形態1～4において、認証方法としてチャレンジレスポンス型のいくつかの例が示されているが、本発明はこれらの例に限られない。例えば、認証側の暗号化ICで乱数を生じし、これをチャレンジデータとして送り、証明側から返送されたレスポンスデータと認証側で生成した参照用のレスポンスデータとを比較する、というチャレンジレスポンス型の別の例であってもよい。

【0099】なお、上記実施の形態1～4において、小さな回路規模で認証と暗号通信を安全に行なう技術を開示したが、安全性の強度とそのために必要な回路規模とはトレードオフの関係にあることは言うまでもない。従って、もしMPUや暗号化IC内に実装できる回路規模に余裕がある場合には、以下の目的のために、データ変換F（）を実行する新たな変換手段を追加導入することで、暗号通信の安全性を強化することができる。

（1）その一つは、平文のチャレンジデータや平文のレスポンスデータが伝送路を流れないようにすることである。

【0100】例えば、図1に示された第1の機器51が第2の機器52を認証する処理シーケンス（ステップ（1）（3）（6）（7））において、以下のように変更新する。ステップ（6）において、第2の暗号化IC56は、分離データRR1をMPU53に送るのではなく、その分離データRR1に所定の変換F（）を施し、その結果得られたデータF（RR1）をMPU53に送る。

【0101】ステップ（7）において、MPU53は、乱数R1と分離データRR1とを比較するのではなく、乱数R1に上記ステップ（6）で用いたものと同じ変換F（）を施し、その結果得られたデータF（R1）と第2の暗号化IC56から送られてきたデータF（RR1）とを比較する。このようにすることで、暗号文C1とその平文の一部RR1とが伝送路を流れることが回避されるので、既知平文攻撃に対する安全性が強化される。

（2）もう一つは、チャレンジデータとそのままデータ転送鍵として用いないようにすることである。

【0102】例えば、図5に示されたステップ（5）において、第1の暗号化IC94は、乱数R1をそのままデータ転送鍵として用いるのではなく、乱数R1に所定の変換F（）を施し、その結果得られたデータF（R1）をデータ転送鍵として用いる。同様に、ステップ（6）において、第2の暗号化IC96は、乱数R1をそのままデータ転送鍵として用いるのではなく、乱数R1に上記ステップ（5）で用いたものと同じ変換F（）を施し、その結果得られたデータF（R1）をデータ転送鍵として用いる。

【0103】このようにすることで、データ転送鍵F(R1)を秘密鍵することができ、暗号通信の安全性が強化される。

(3) さらにもう一つは、結合処理を複雑にすることである。例えば、図1に示されたステップ(9)において、第1の暗号化IC54は、乱数R3と分離データRR4とを単に桁方向に結合するのではなく、これらR3、RR4に所定の変換F()を施し、その結果得られたデータF(R3、RR4)をデータ転送鍵Kとする。

【0104】同様に、ステップ(10)において、第2の暗号化IC56は、乱数R4と分離データRR3とを単に桁方向に結合するのではなく、これらR4、RR3に上記ステップ(9)で用いたものと同じ変換F()を施し、その結果得られたデータF(R3、RR4)をデータ転送鍵Kとする。このようにすることで、データ転送鍵Kの生成手順が複雑化され、暗号通信の安全性が強化される。

(具体的な通信システムへの応用例) 以上のように、本発明に係る暗号化装置は、規模の小さな暗号化ICを備え、機器間通信の安全性を確保するための必要最小限の機能を持っている。従って、本暗号化装置は、秘密通信が必要とされ、かつ、小型であることが要求される通信機器、例えば、携帯電話機やデジタル著作権物を扱うマルチメディア関連機器等に好適な装置である。

【0105】図7は、本発明に係る暗号化装置の具体的な通信システムへの応用例を示す図であり、映画等のデジタル著作権物の再生システムの概観を示す。このシステムは、上記実施形態における第1の機器に対応する光ディスクドライブ装置110と第2の機器に対応する映像再生装置111とそれらを接続するSCS1ケーブル116等からなる。光ディスクドライブ装置110で読み出した圧縮映像データを暗号化して映像再生装置111に転送し、そこで映像再生するシステムである。

【0106】図8は、光ディスクドライブ装置110の構成を示すブロック図である。光ディスクドライブ装置110は、装置全体の制御を行うMPU124と、映像再生装置111との通信インターフェースであるSCS1コントローラ121と、光ヘッド125を制御して光ディスク115から映像データを読み出し制御する読み出し制御部122と、上述の実施形態1〜4における第1の機器の暗号化ICに相当する暗号化IC123とからなり、映像再生装置111が正当な機器であることを認証した後に、光ディスク115に記録された映像データを読み出して暗号化IC123において暗号化し、SCS1ケーブル116を介して映像再生装置111に転送する。

【0107】図9は、光ディスクドライブ装置110の内部に実装される回路基板の概観を示す図である。暗号化IC123は、1個のシリコン基板に形成されたLSIであり、プラスチックでモールドされたフラットパッ

ケージの形状をしている。図10は、映像再生装置111の構成を示すブロック図である。映像再生装置111は、装置全体の制御を行うMPU131と、光ディスクドライブ装置110との通信インターフェースであるSCS1コントローラ130と、上述の実施形態1〜4の第2の機器の暗号化ICに相当する暗号化IC132と、暗号化IC132で復号された圧縮映像データの伸長を行うMPEGデコーダ133と、伸長された映像データをアナログ映像信号に変換してCRT112及びスピーカ114に映像出力するAV信号処理部134とから構成される。

【0108】本発明に係る暗号化装置をこのような映像再生システムに適用することで、光ディスク115に記録されたデジタル著作権物は不正コピー等から保護され、マルチメディア関連製品の流通市場における健全な発展が期待できる。

【0109】

【発明の効果】以上の説明から明らかなように、本発明に係る暗号化装置は、データ転送鍵の共有化とそのデータ転送鍵を用いた暗号通信を行なう機器に備えられる暗号化装置であって、前記データ転送鍵の共有化のための第1乱数を生成する第1乱数生成手段と、前記第1乱数生成手段により生成された第1乱数を保持する第1乱数保持手段と、前記第1乱数生成手段により生成された第1乱数を前記暗号通信の相手機器に送信する第1送信手段と、前記第1乱数保持手段に保持された第1乱数を用いて時変の前記データ転送鍵を生成するデータ転送鍵生成手段と、暗号通信の対象となる転送データに対して前記データ転送鍵を用いて暗号化する転送データ暗号化手段とを備え、前記第1乱数生成手段、前記第1乱数保持手段、前記データ転送鍵生成手段及び前記転送データ暗号化手段は、1個のIC内の回路で実現され、前記第1乱数保持手段は、前記ICの外部からアクセスできない領域に前記第1乱数を保持することを特徴とする。

【0110】これにより、データ転送鍵の生成に直接関連する第1乱数は外部からアクセスできない暗号化ICの内部に保持されるので、時変のデータ転送鍵は各機器に安全に共有され、暗号通信が行われる。また、暗号化ICは、機器間通信の安全性を確保するための必要最小限の機能を持つので、小さな回路で実現することができる。

【0111】ここで、前記暗号化装置はさらに、前記第1乱数生成手段により生成された第1乱数を暗号化する第1暗号化手段を備え、前記第1暗号化手段は、前記IC内の回路で実現され、前記第1送信手段は、前記第1暗号化手段で暗号化された第1乱数を前記相手機器に送信するとすることもできる。これにより、第3者はデータ転送鍵の生成に直接関連する第1乱数を知ることができなくなるので、データ転送鍵の秘密性が維持され、たとえ暗号アルゴリズム及びその逆変換アルゴリズムが知

られたとしても暗号通信は維持される。

【0112】ここで、前記機器は、チャレンジレスポンス型の認証プロトコルに基づく通信により相互に前記相手機器が正当な機器であることを認証し合うものであり、前記暗号化装置はさらに、前記相手機器に送信するチャレンジデータ用の第2乱数を生成する第2乱数生成手段と、前記チャレンジデータに対して前記相手機器から返信されてきたレスポンスデータと前記第2乱数とが一致するか否かを判断し、一致した場合に前記相手機器は正当な機器であると認証する認証手段とを備え、前記データ転送鍵生成手段は、前記認証がなされた場合に前記データ転送鍵を生成するとすることもできる。

【0113】これにより、機器間の相互認証が成功したときに同時に正規のデータ転送鍵が生成されることになり、秘密通信の安全性が向上される。ここで、前記第2乱数生成手段及び前記認証手段は、前記IC外の回路で実現されているとすることもできる。これにより、通信システムの安全性に関連しない部分、即ち、データ転送鍵の生成に直接関連しない処理部は暗号化ICの外に設けられるので、暗号化ICの規模が不要に大きくなることが抑制される。

【0114】ここで、前記暗号化装置はさらに、前記相手機器から送られてきた暗号化された結合データを復号化する復号化手段と、復号化された結合データをレスポンスデータに相当する第1分離データと残る第2分離データとに分離する分離手段と、前記第1分離データを前記相手機器に返信する第2送信手段とを備え、前記第1暗号化手段は、前記第1乱数と前記第2乱数とを結合し、その結果得られた結合データを暗号化し、前記データ転送鍵生成手段は、前記第1乱数と前記第2分離データとを結合することにより、前記データ転送鍵を生成し、前記復号化手段及び前記分離手段は、前記IC内の回路で実現されているとすることもできる。

【0115】また、前記暗号化装置はさらに、前記第2乱数をチャレンジデータとして前記相手機器に送信する第2送信手段と、前記相手機器から送られてきた暗号化された結合データを復号化する復号化手段と、復号化された結合データをレスポンスデータに相当する第1分離データと残る第2分離データとに分離する分離手段とを備え、前記認証手段は、前記第1分離データを前記相手機器から返信されてきたレスポンスデータとして前記判断及び認証をし、前記第1暗号化手段は、前記相手機器から返信されてきたチャレンジデータと前記第1乱数とを結合し、その結果得られた結合データを暗号化し、前記データ転送鍵生成手段は、前記第1乱数と前記第2分離データとを結合することにより、前記データ転送鍵を生成し、前記復号化手段及び前記分離手段は、前記IC内の回路で実現されているとすることもできる。

【0116】これにより、機器間通信の安全性を確保するための必要最小限の機能を持ち、規模の小さな暗号化

ICを備えた暗号化装置が実現される。ここで、前記転送データ暗号化手段による暗号化のアルゴリズムは、前記第1暗号化手段及び前記復号化手段の少なくとも一つのものと同じであることを特徴とするとしてもできる。

【0117】これにより、転送データ暗号化手段と第1暗号化手段や復号化手段を1個の変換器で兼用して実装することが可能となるので、暗号化ICの回路規模が削減される。ここで、前記転送データ暗号化手段による暗号化のアルゴリズムは、前記第1暗号化手段及び前記復号化手段のいずれのものとも異なり、かつ、いずれのものよりも簡易であるとしてもできる。

【0118】これにより、転送データのサイズが大きいために何度もその暗号化を繰り返すような場合であっても、暗号化のためにデータ転送時間が大幅に長くなってしまふという不具合が回避される。ここで、前記転送データ暗号化手段は、前記転送データを一定長のブロックに区切り、各ブロックに対して前記データ転送鍵の対応する部分を用いて暗号化するとすることもできる。

【0119】これにより、データサイズの大きい転送データの暗号通信に対しても、本暗号化装置を適用することが可能となる。ここで、前記転送データ暗号化手段は、前記ブロックと前記データ転送鍵の対応する部分との排他的論理和をとることにより、前記暗号化を行なうとすることもできる。

【0120】これにより、簡易な論理回路で転送データ暗号化手段を実現することが可能となる。ここで、前記第1暗号化手段での暗号と前記復号化手段での復号化とは、同一の変換アルゴリズムであるとしてもできる。これにより、第1暗号化手段と復号化手段を1個の変換器で兼用して実装することが可能となり、暗号化ICの回路規模が削減される。

【0121】ここで、前記第1暗号化手段及び前記復号化手段は、予め前記IC内に保持された鍵データを用いて前記暗号化及び復号化を行い、その鍵データの一部は、前記IC内のマスクROM領域に格納され、残る一部は、前記IC内の追記ROM領域に格納されているとすることもできる。これにより、認証鍵をマスクROMのみで構成した場合における欠点と、追記ROMのみで構成した場合における欠点と補うことが可能となる。

【0122】ここで、前記機器は、チャレンジレスポンス型の認証プロトコルに基づく通信により相互に前記相手機器が正当な機器であることを認証し合うものであり、前記暗号化装置はさらに、前記チャレンジデータに対して前記相手機器から送られてきた暗号化された結合データを復号化する復号化手段と、復号化された結合データをレスポンスデータに相当する第1分離データと残る第2分離データとに分離する分離手段と、前記第1乱数と前記第1分離データとが一致するか否かを判断し、一致した場合に前記相手機器は正当な機器であると認証

する認証手段と、前記認証がなされた場合に前記第2分離データを暗号化する第2暗号化手段と、暗号化された前記第2分離データをレスポンスデータとして前記相手機器に返信する第2送信手段とを備え、前記データ転送鍵生成手段は、前記第1乱数と前記第2分離データとを結合することにより、前記データ転送鍵を生成し、前記復号化手段、前記分離手段及び前記第2暗号化手段は、前記1C内の回路で実現されているとすることもできる。

【0123】これにより、乱数をつだけ生成し、それを認証用とデータ転送鍵の生成用の両方の目的に使用しているため、暗号化装置での乱数生成のための回路規模が軽減される。また、暗号化1Cの内部において認証のための乱数生成と比較処理を行っているため、暗号通信の安全性が高められる。

【0124】また、本発明は、データ転送鍵の共有化とそのデータ転送鍵を用いた暗号通信を行なう送信機及び受信機から構成される通信システムであって、それら送信機及び受信機が、それぞれ上記構成を備えるとしてもできる。これにより、送信機及び受信機間で相互認証が行われると共にデータ転送鍵が生成されること、データ転送鍵の生成に直接関連する乱数はそのままでは送受信されないこと、及び、データ転送鍵の生成に直接関連する2つの乱数はそれぞれ送信機及び受信機から提供されたものであることから、規模の小さな暗号化1Cを用いて実現するのに好適であり、かつ、安全性の高い暗号通信システムが実現される。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態に係る暗号化装置の処理シーケンスを示す図である。

【図2】図1に示された第1の暗号化1C54のハードウェア構成を示すブロック図である。

【図3】本発明の第2の実施の形態に係る暗号化装置の処理シーケンスを示す図である。

【図4】本発明の第3の実施の形態に係る暗号化装置の処理シーケンスを示す図である。

【図5】本発明の第4の実施の形態に係る暗号化装置の処理シーケンスを示す図である。

【図6】図5に示された第1の暗号化1C94のハードウェア構成を示すブロック図である。

【図7】本発明に係る暗号化装置の具体的な通信システムへの適用例を示す図である。

【図8】図7に示された光ディスクドライブ装置110の構成を示すブロック図である。

【図9】同光ディスクドライブ装置110の内部に実装される回路基板の概観を示す図である。

【図10】図7に示された映像再生装置111の構成を示すブロック図である。

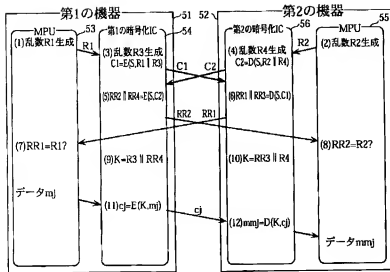
【図11】第1の従来技術に係る一方認証の処理シーケンスを示す図である。

【図12】第2の従来技術に係る双方認証の処理シーケンスを示す図である。

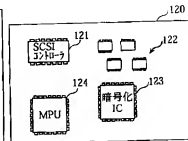
【符号の説明】

51、71、81、91	第1の機器
52、72、82、92	第2の機器
53、73、83、93	第1の機器のMPU
54、74、84、94	第1の暗号化1C
55、75、85、95	第2の機器のMPU
56、76、86、96	第2の暗号化1C
59	データ転送鍵K生成部
60、101	乱数生成部
61、100	外部I/F部
62、102	乱数格納部
63	結合部
64、103	認証鍵S格納部
65、66、68、104、105、107	スイッチ
67、106	E関数
69	分離部
70	データ転送鍵K格納部
108	比較部
110	光ディスクドライブ装置
111	映像再生装置
121	SCSIコントローラ
122	制御部
123	暗号化1C
124	MPU
125	光ヘッド
130	SCSIコントローラ
131	MPU
132	暗号化1C
133	MPEGデコーダ
134	AV信号処理部

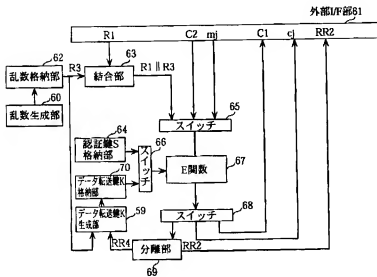
【図1】



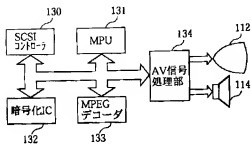
【図9】



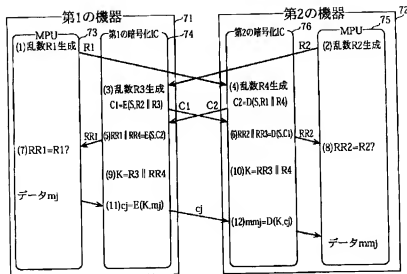
【図2】



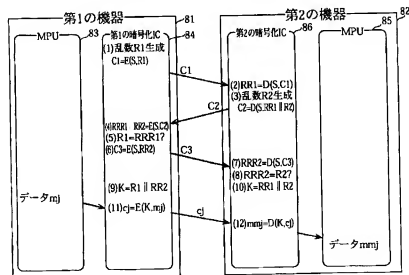
【図10】



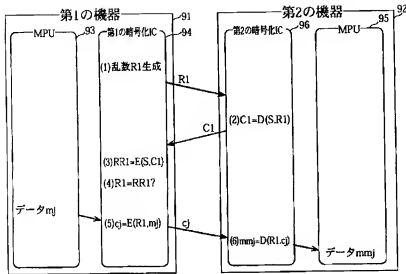
【図3】



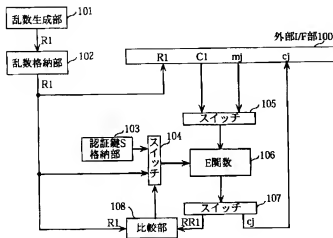
【図4】



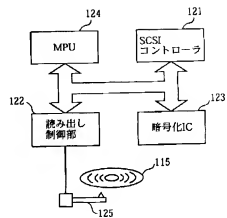
【図5】



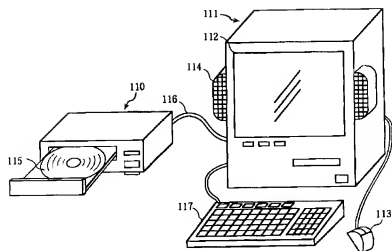
【図6】



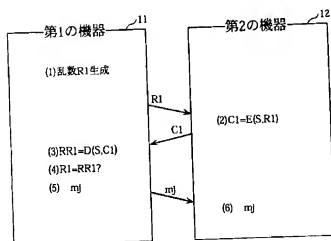
【図8】



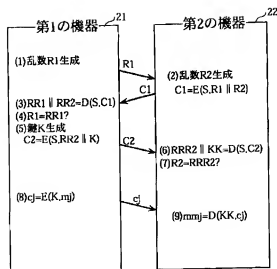
【図7】



【図11】



【図12】



フロントページの続き

(51) Int. Cl. 6

識別記号 庁内整理番号

F I
H O 4 L 9/00技術表示箇所
6 7 5 A